NetIQ® eDirectory™ 8.8 SP8

Handbücher zur Fehlersuche

September 2013



Rechtliche Hinweise

Inhalt

Info zu diesem Handbuch und zur Bibliothek

Das *Handbuch zur Fehlersuche* enthält Informationen zur Behebung von Problemen mit NetIQ eDirectory (eDirectory).

Die neueste Version des *Handbuchs zur Fehlersuche für NetIQ eDirectory 8.8 SP8* finden Sie auf der Website der NetIQ eDirectory 8.8-Onlinedokumentation.

Zielgruppe

Dieses Handbuch richtet sich an Netzwerkadministratoren.

Weitere Informationen in der Bibliothek

Die Bibliothek enthält folgende Informationsressourcen:

XDASv2-Administrationshandbuch

Beschreibt die Konfiguration und Arbeit mit XDASv2 zur Prüfung von eDirectory und NetIQ Identity Manager.

Installationshandbuch

Beschreibt die Installation von eDirectory. Das Handbuch richtet sich an Netzwerkadministratoren.

Verwaltungshandbuch

Beschreibt die Verwaltung und Konfiguration von eDirectory.

Handbuch zu neuen Funktionen

Beschreibt die neuen Funktionen von eDirectory.

Optimierungshandbuch für Linux-Plattformen

Beschreibt, wie eDirectory auf Linux-Plattformen mittels Analyse und Feinabstimmung optimiert werden kann, um in allen Bereitstellungen eine bessere Leistung zu erzielen.

Diese Handbücher sind auf der NetIQ eDirectory 8.8-Dokumentationswebsite verfügbar.

Informationen zur eDirectory-Verwaltungsfunktion finden Sie im *NetIQ iManager 2.7-Administrationshandbuch*.

Info zu NetIQ Corporation

NetIQ ist ein globaler Hersteller von Unternehmenssoftware. Unser Blickpunkt liegt auf drei besonderen Herausforderungen, die Sie in Ihrer Umgebung meistern müssen: Änderungen, Komplexität und Risiken. Unser Ziel ist es, Sie dabei zu unterstützen.

Unser Standpunkt

Sich an Änderungen anzupassen und Komplexität und Risiken zu beherrschen ist nichts Neues

Unter den verschiedenen Herausforderungen, denen Sie gegenüberstehen, beeinflussen diese drei Punkte sicherlich am meisten Ihre Möglichkeiten, Ihre physikalischen, virtuellen und Cloud-Umgebungen sicher zu messen, zu überwachen und zu verwalten.

Kritische Geschäftsservices schneller und besser bereitstellen

Wir sind davon überzeugt, dass IT-Organisationen über eine möglichst große Kontrolle verfügen müssen, um eine zeitgerechte und kostenwirksame Servicebereitstellung zu ermöglichen. Der von Änderungen und Komplexität ausgehende, kontinuierliche Druck steigt ständig, weil sich die Unternehmen ständig ändern und die erforderlichen Technologien zur Verwaltung der Änderungen immer komplexer werden.

Unsere Philosophie

Intelligente Lösungen entwickeln, nicht einfach Software

Um zuverlässige Lösungen für die Kontrolle anbieten zu können, stellen wir erst einmal sicher, dass wir das Szenario, in dem Unternehmen wie das Ihre täglich arbeiten, gründlich verstehen. Nur so können wir praxistaugliche, intelligente IT-Lösungen entwickeln, die nachweisbar messbare Ergebnisse liefern. Und das ist für uns wesentlich bereichernder, als einfach eine Software zu verkaufen.

Ihr Erfolg ist unsere Leidenschaft

Ihr Erfolg ist der Wegweiser für unser Geschäft. Wir wissen, dass Sie von der Produktkonzeption bis hin zur Bereitstellung IT-Lösungen benötigen, die richtig funktionieren und nahtlos mit Ihren vorhandenen Investitionen integriert werden können. Sie benötigen fortlaufenden Support, Schulungen nach der Bereitstellung und jemanden, mit dem Sie unkompliziert arbeiten können. Ihr Erfolg ist auch unser Erfolg.

Unsere Lösungen

- Identitäts- und Zugriffsregelung
- Zugriffsverwaltung
- Sicherheitsverwaltung
- System- und Anwendungsverwaltung

- Workload-Management
- Serviceverwaltung

Anfragen an die Verkaufsunterstützung

Bei Fragen zu Produkten, Preisen und Funktionen wenden Sie sich an Ihren Händler vor Ort. Wenn dies nicht möglich ist, wenden Sie sich an unser Verkaufsunterstützungsteam.

Weltweit:	www.netiq.com/about_netiq/officelocations.asp
Vereinigte Staaten und Kanada:	1-888-323-6768
Email:	info@netiq.com
Website:	www.netiq.com

Kontakt zum technischen Support

Bei spezifischen Produktproblemen, wenden Sie sich an unseren technischen Support.

Weltweit:	www.netiq.com/support/contactinfo.asp
Nord- und Südamerika:	1-713-418-5555
Europa, Naher Osten und Afrika:	+353 (0) 91-782 677
Email:	support@netiq.com
Website:	www.netiq.com/support

Kontakt zum Dokumentationssupport

Wir möchten Ihnen stets eine nützliche, aussagekräftige Dokumentation an die Hand geben. Wenn Sie uns einen Verbesserungsvorschlag mitteilen möchten, nutzen Sie die Schaltfläche **Kommentar hinzufügen**, die unten auf jeder Seite der unter www.netiq.com/documentation veröffentlichten HTML-Versionen unserer Dokumentation verfügbar ist. Sie können Verbesserungsvorschläge auch per Email an Documentation-Feedback@netiq.com senden. Wir freuen uns auf Ihre Rückmeldung.

Kontakt zur Online-Benutzer-Community

Qmunity, die NetIQ-Online-Community, ist ein Netzwerk zur Zusammenarbeit mit anderen NetIQ-Benutzern und -Experten. Qmunity bietet Ihnen aktuellste Informationen, nützliche Links zu hilfreichen Ressourcen und Kontakt zu NetIQ-Experten, damit Sie über alle Voraussetzungen verfügen, um das meiste aus den IT-Investitionen zu holen, auf die Sie sich verlassen. Weitere Informationen hierzu finden Sie im Internet unter http://community.netiq.com.

1 Fehlercodes auflösen

Eine vollständige Liste der Fehlercodes in eDirectory und entsprechende Erläuterungen finden Sie auf der NetIQ Fehlercodes-Website (http://www.novell.com/documentation/nwec/).

2 Installation und Konfiguration

2.1 Installation

Dieser Abschnitt enthält Informationen zu verschiedenen Problemen, die während der Installation von eDirectory 8.8 auftreten können, und Tipps zur Behebung dieser Probleme.

2.1.1 Schwerwiegender Fehler bei der Schemasynchronisierung, wenn auf einem SLES 11-Computer ein zweiter eDirectory-Server im Baum installiert wird

Konfigurieren Sie einen eDirectory-Baum und installieren Sie einen weiteren Server im Baum. Wählen Sie in beiden Fällen die Option zur Verwendung aller verfügbaren Schnittstellen aus. Verwenden Sie für beide Server die gleichen Schnittstellen. Beispiel: 127.0.0.2. Starten Sie DSTrace auf dem ersten Server mit den Optionen SCMA, SKLK und SYNC.

2.1.2 Fehler bei der Installation

- Prüfen Sie im Verzeichnis `/var/adm/messages` auf folgende Fehlermeldung:

```
Unable to bind to SLP Multicast Address. Multicast route not added?
```

Diese Meldung wird angezeigt, wenn der Linux- oder Solaris-Computer nicht für eine Multicast-Routing-Adresse konfiguriert ist.

Fügen Sie die Multicast-Routing-Adresse hinzu und starten Sie den Daemon slpuasa erneut.

- Wenn die Fehlermeldung `-632: Fehlerbeschreibung Systemfehler` während der Installation angezeigt wird, beenden Sie den Installationsvorgang.

  Legen Sie für den Parameter `n4u.base.slp.max-wait` in der Datei `/etc/opt/novell/eDirectory/conf/nds.conf` einen höheren Wert fest, beispielsweise 50. Starten Sie dann den Installationsvorgang neu.
- Gehen Sie folgendermaßen vor, wenn während der Installation die Fehlermeldung `Tree Name Not Found` (Baumname nicht gefunden) angezeigt wird:

1. Überprüfen Sie, ob Multicast-Routing auf dem Solaris-Host, auf dem Sie das Produkt installieren, aktiviert ist.
2. Geben Sie die IP-Adresse des Masterservers der Baumpartition an.

2.1.3 Installation dauert lange

Wenn die Installation von eDirectory in einem vorhandenen Baum einen langen Zeitraum in Anspruch nimmt, wechseln Sie zum DSTrace-Bildschirm auf dem Server. Wenn die Meldung `-625 Transportfehler` angezeigt wird, muss der Adressen-Cache zurückgesetzt werden.

Der Cache-Speicher für Adressen wird mit folgendem Befehl an der Systemkonsole zurückgesetzt:

```
set dstrace = *A
```

2.1.4 Fehler bei der eDirectory-Installation für Containerverwalter

Das Installationsprogramm für eDirectory 8.8 unterstützt Installationen durch Administratoren mit Supervisor-Rechten am Container, in dem sich der Server befindet. Damit dies möglich ist, muss der erste Server, auf dem eDirectory 8.8 installiert wird, über Supervisor-Rechte zum [Stammverzeichnis] verfügen, um das Schema zu erweitern. Für weitere Server ist es anschließend nicht erforderlich, über Rechte am [Stammverzeichnis] zu verfügen. Je nachdem, auf welcher Plattform eDirectory 8.8 zuerst installiert wird, können jedoch möglicherweise nicht alle Schemen erweitert werden. Für die nachfolgenden Serverinstallationen auf anderen Plattformen sind Supervisor-Rechte zum [Stammverzeichnis] erforderlich.

Wenn eDirectory 8.8 auf mehreren Plattformen installiert wird, vergewissern Sie sich, dass Sie über Supervisor-Rechte zum [Stammverzeichnis] des jeweils ersten Servers JEDER Plattform verfügen, auf der eDirectory installiert wird. Wenn eDirectory 8.8 beispielsweise zuerst auf einem unter Linux ausgeführten Server, dann aber auch auf einem Solaris-Server installiert werden soll, muss der jeweils erste Server jeder Plattform über Supervisor-Rechte für das [Stammverzeichnis] verfügen. Zusätzliche Server jeder Plattform benötigen lediglich Containerverwalterrechte am Container, in dem der Server installiert wird.

Weitere Informationen finden Sie in der Lösung NOVL83874 (http://support.novell.com/docs/Tids/Solutions/10073723.html) im *eDirectory 8.7.x-Readme-Nachtrag*.

2.1.5 Fehler bei der NICI-Installation - 1497

Eine Warnmeldung zu einem Fehler bei der Initialisierung der NetIQ International Cryptographic Infrastructure (NICI) bedeutet, dass die Datei `NFK` falsch ist. Vergewissern Sie sich, dass Sie über die richtige `NFK`-Datei verfügen. Dieses Problem tritt auf Linux-Plattformen nicht auf, weil die `NFK`-Datei standardmäßig Bestandteil des NICI-Pakets ist.

2.1.6 Benennen von Objekten

Wenn Sie bei der Benennung von Objekten Sonderzeichen verwenden, wird die Fehlermeldung `-671 Keine solche Überordnung` angezeigt. Vermeiden Sie beim Benennen von Objekten die Verwendung folgender Sonderzeichen:

\ /, * ? .

2.1.7 NICI wird im Servermodus unter Windows nicht installiert

Das Dialogfeld „Eigenschaften" der Datei `NICIFK` enthält eine Registerkarte mit der Bezeichnung „Sicherheit". Wenn das Feld für die Gruppen- bzw. Benutzernamen keine Namen enthält, tritt dieses Problem auf.

Dieses Problem lässt sich folgendermaßen umgehen:

1 Entfernen Sie die Datei `NICIFK`.

   Sie befindet sich im Verzeichnis `C:/Windows/system32/novell/nici`, wenn das Systemstammverzeichnis `C:/Windows/system32` lautet. Wenn das Systemstammverzeichnis `F:/Windows/system32` ist, befindet sich die Datei im Verzeichnis `F:/Windows/system32/novell/nici`.

2 Installieren Sie eDirectory.

2.1.8 Bei der Aufrüstung der Tarball-Datei tritt ein Fehler auf und die Fehlermeldung „Cannot open or remove a file containing a running program" (Datei, die ein ausgeführtes Programm enthält, kann nicht geöffnet oder entfernt werden) wird angezeigt

Wenn während einer Tarball-Aufrüstung in AIX in der Dateikopierphase die Fehlermeldung `Cannot open or remove a file containing a running program` (Datei, die ein ausgeführtes Programm enthält, kann nicht geöffnet oder entfernt werden) angezeigt ist, umgehen Sie das Problem folgendermaßen:

1 Führen Sie `/usr/sbin/slibclean` als root-Benutzer aus.

2 Setzen Sie die Aufrüstung von der Dateikopierphase fort.

2.1.9 Problem mit eDirectory und YUM

Wenn Sie eDirectory 8.8 SP6 oder höher auf einem Red Hat Enterprise Linux-Server installieren, auf dem der YUM-Paketmanager installiert ist, tritt bei der Verwendung von YUM möglicherweise ein Fehler auf.

Sowohl YUM als auch eDirectory 8.8 verwenden die Bibliothek `libexpat.so.0`. Wenn Sie YUM mit einer oder mehreren Optionen ausführen, gibt YUM einen Fehler in der Konsole zurück. Sie können dieses Problem umgehen, indem Sie mit einem Texteditor folgende Zeile in der Datei `/etc/ld.so.conf.d/novell-NDSbase.conf` auskommentieren und dann `ldconfig` ausführen:

```
/opt/novell/eDirectory/lib64
```

Nachdem Sie die Zeile auskommentiert und `ldconfig` ausgeführt haben, führen Sie bei jedem Start von eDirectory folgenden Befehl in einem Terminalfenster aus:

```
source /opt/novell/eDirectory/bin/ndspath
```

Starten Sie eDirectory im gleichen Terminal neu. ndspath löst die erforderlichen Pfadabhängigkeiten auf.

2.1.10 Leistungsprobleme beim Ausführen von eDirectory mit BTRFS

Wenn Sie eDirectory auf einem SLES-Server innerhalb eines BTRFS-Dateisystems installieren, können bei LDAP-Operationen oder bei der Verwendung der NetIQ Import Conversion Export Utility (ICE) Leistungsprobleme auftreten. Aus Leistungsgründen wird empfohlen, das ext3-Dateisystem für den eDirectory-Server zu verwenden.

2.2 Konfiguration

Dieser Abschnitt enthält Informationen zu Problemen, die während der Konfiguration von eDirectory 8.8 auftreten können.

2.2.1 Loopback-Verweise werden von einem Verzeichnisserver zurückgegeben

Wenn eDirectory zur Überwachung von Loopback-Adressen konfiguriert ist, werden die Loopback-Adressen gespeichert und an die Clients zurückgegeben, wenn sie Suchen und andere Operationen ausführen. Die Verweise sind für Clients, die einen Verbindungsversuch von einem anderen

Computer als dem Server ausführen, nicht zutreffend. Daher tritt beim Verbindungsversuch der Clients mit diesen Loopback-Verweisen ein Fehler auf. Die anderen vom Server zurückgegebenen Verweise funktionieren jedoch für diese Clients.

Der Versuch, zu jedem Loopback-Verweis eine Verbindung aufzubauen, und dann die richtigen Verweise auszuwählen, kann die Leistung der Clients beeinträchtigen.

So umgehen Sie das Problem: Wählen Sie nur eine Schnittstelle aus, mit der eDirectory kommunizieren kann. Wählen Sie während der Installation nicht die Loopback-Schnittstellen aus.

2.2.2 -632: Fehler bei Baumnamensuche während der Konfiguration von eDirectory 8.8 unter Linux

Bei der Konfiguration von eDirectory 8.8 unter Linux kann der Fehler „Tree name lookup failed: -632“ (Fehler bei der Baumnamensuche) auftreten. Gehen Sie wie folgt vor, um dieses Problem zu beheben:

1. Stellen Sie sicher, dass Sie SLP nach der Installation des SLP-Pakets folgendermaßen manuell neu starten:

   ```
   /etc/init.d/slpuasa start
   ```

2. Stellen Sie sicher, dass Sie SLP nach der Deinstallation des SLP-Pakets folgendermaßen manuell stoppen:

   ```
   /etc/init.d/slpuasa stop
   ```

2.2.3 Hinzufügen neuer Server

Sie können einen neuen Server nicht in einen Kontext hinzufügen, wenn der vollqualifizierte Domänenname länger als 255 Zeichen ist. Die Längenbeschränkung gilt für den vollqualifizierten Domänennamen und nicht für die Kontextlänge. Der vollqualifizierte Domänenname eines Objekts darf höchstens 255 Zeichen lang sein.

2.2.4 Ausschluss des DIB-Verzeichnisses von Sicherungs- und Virenschutzprozessen

Nach der Installation von eDirectory sollten Sie die Umgebung so konfigurieren, dass das DIB-Verzeichnis auf dem eDirectory-Server von allen Virenschutz- und Sicherungssoftwareprozessen ausgeschlossen wird. Wenn Sie das DIB-Verzeichnis nicht von Prozessen dieser Art ausschließen, können beschädigte DIB-Dateien oder Fehler der Art `-618 FFFFFD96 INCONSISTENT DATABASE` (Inkonsistente Datenbank) auftreten.

Sichern Sie das DIB-Verzeichnis mit dem eDirectory -Sicherungswerkzeug. Weitere Informationen zum Sichern von eDirectory finden Sie unter „Sichern und Wiederherstellen von NetIQ eDirectory“ im *NetIQ eDirectory 8.8 SP8-Administrationshandbuch*.

2.2.5 „ndsconfig“ in eDirectory zeigt auf 32-Bit-Plattformen von RHEL einen Fehler an

„ndsconfig“ in eDirectory zeigt auf 32-Bit-RHEL-Plattformen folgenden Fehler an:

```
/opt/novell/eDirectory/lib/libsal.so.1.0.0
```

```
error while loading shared libraries: /opt/novell/lib/libccs2.so: cannot
restore segment prot after reloc: Permission denied
```

Führen Sie die folgenden Befehle aus, um das Problem zu umgehen:

```
chcon -t textrel_shlib_t '/opt/novell/eDirectory/lib/libsal.so.1.0.0'
```

```
chcon -t textrel_shlib_t '/opt/novell/lib/libccs2.so.2.7.6'
```

2.2.6 IP-AG-Zertifikat wird auf 64-Bit-Plattformen von SLES 11 nicht erstellt

Dieses Problem betrifft Szenarien, in denen für eDirectory 8.8 SP8 sowohl IPv4 als auch IPv6 konfiguriert ist und nur für eine Version (beispielsweise nur für IPv4) ein Eintrag in der Datei `/etc/hosts` vorhanden ist, während die andere Schnittstelle über einen Remote-Computer zugreifbar ist. Wenn Sie eDirectory zur Überwachung beider IPs konfigurieren, wird das IP-AG-Zertifikat nur für die IP generiert, die in der Datei `/etc/hosts` aufgeführt ist. In diesem Beispiel wird das Zertifikat also nur für IPv4 generiert.

2.3 Aufrüstung

- Abschnitt 2.3.1, „Fehler bei der Aufrüstung, wenn der Mountpunkt auf „/var/opt/novell/eDirectory/data“ festgelegt ist“, auf Seite 20
- Abschnitt 2.3.2, „Bei der Aufrüstung von eDirectory nach dem Anwenden eines Patch wird die Patch-Version auf Windows-Systemen nicht entfernt“, auf Seite 21

2.3.1 Fehler bei der Aufrüstung, wenn der Mountpunkt auf „/var/opt/novell/eDirectory/data“ festgelegt ist

Beim Aufrüsten von eDirectory über den Befehl `ndsconfig upgrade` tritt ein Fehler auf, wenn der Mountpunkt auf `/var/opt/novell/eDirectory/data` festgelegt ist. Die Aufrüstung wird angehalten und folgende Fehlermeldung wird angezeigt:

```
ERROR: Unable to check if the directory "/var/opt/novell/eDirectory/data_upg_bak"
already exists. If the directory exists, delete it and execute `ndsconfig upgrade -
-config-file /etc/nds.conf`to restart the upgrade operation.
```

Das Problem tritt auf, weil das Verzeichnis `/var/opt/novell/eDirectory/data` während der Aufrüstung in `/var/opt/novell/eDirectory/data_upg_bak` umbenannt wird, damit keine Kundendaten verloren gehen. In diesem Fall ist das Verzeichnis `/var/opt/novell/eDirectory/data` der Mountpunkt, der nicht umbenannt werden kann.

Führen Sie einen der folgenden Schritte aus, um dieses Problem zu umgehen:

- Ändern Sie den Mountpunkt zu `/var/opt/novell/eDirectory`.
- Führen Sie Folgendes aus:
  1. Erstellen Sie das Verzeichnis `/var/opt/novell/eDirectory/data_upg_bak`.
  2. Verschieben Sie die Dateien von `/var/opt/novell/eDirectory/data` zu `/var/opt/novell/eDirectory/data_upg_bak`.

  WICHTIG: Lassen Sie das Verzeichnis `/var/opt/novell/eDirectory/data` leer, um eine reibungslose Aufrüstung zu gewährleisten.

2.3.2 Bei der Aufrüstung von eDirectory nach dem Anwenden eines Patch wird die Patch-Version auf Windows-Systemen nicht entfernt

Wenn Sie eDirectory nach dem Anwenden eines Patch aufrüsten, wird nicht die Patch-Version aufgerüstet, sondern die Basisversion des Produkts.

Das Problem wurde in folgenden Aufrüstungsszenarien beobachtet und reproduziert:

Tabelle 2-1 *eDirectory-Versionen*

Basisproduktversion	Patch-Version	Aufgerüstete Version
eDirectory 873	87310	eDirectory 88 SP3
eDirectory 873		eDirectory 88 SP3
eDirectory 873		eDirectory 873 SP10
eDirectory 88 SP6	beliebiger Patch	eDirectory 88 SP8

Dieses Problem tritt auf, weil die Installationsprogramme für eDirectory und für Patches in Windows getrennt sind. Das Basisprodukt von eDirectory wird über das NIS-Framework installiert; Patches wie eDirectory 8.8 SP5 Patch 2 werden unter Verwendung des Nulsoft Installer Script (NSIS) installiert. Da es sich um verschiedene Installationsprogramme handelt, wird nur die Basisversion des Produkts aufgerüstet, nicht der mit NSIS installierte Patch.

Um das Problem zu umgehen, entfernen Sie bei der Aufrüstung den Registrierungseintrag des Patch (zum Beispiel: eDirectory 8.7.3 SP9/eDirectory 8.7.3 SP10/eDirectory 8.8 SP5 patch 2 und eDirectory 8.8 SP5 patch 3).

2.4 Mehrere Instanzen

Beim Arbeiten mit mehreren Instanzen von eDirectory können folgende Probleme auftreten:

- Abschnitt 2.4.1, „Wenn die erste Instanz ausfällt, funktioniert HTTP nicht“, auf Seite 21
- Abschnitt 2.4.2, „eDirectory überwacht nicht alle konfigurierten Schnittstellen“, auf Seite 21

2.4.1 Wenn die erste Instanz ausfällt, funktioniert HTTP nicht

Wenn eDirectory unter Linux auf einer Maschine mit mehreren NIC-Karten konfiguriert, HTTP an mehr als eine Schnittstelle gebunden ist und die erste Schnittstelle ausfällt, kann von den verbleibenden Schnittstellen aus nicht auf HTTP zugegriffen werden.

Dies liegt daran, dass die verbleibenden Schnittstellen die Anforderung an die erste Schnittstelle umadressieren, die erste Schnittstelle jedoch heruntergefahren ist.

Um dieses Problem zu umgehen, starten Sie eDirectory neu, wenn die erste Schnittstelle ausfällt.

2.4.2 eDirectory überwacht nicht alle konfigurierten Schnittstellen

Stellen Sie sicher, dass alle Schnittstellen, auf denen eDirectory konfiguriert ist, ausgeführt werden und verbunden sind.

2.4.3 ndsd kehrt zum Standardport zurück, wenn die angegebene Schnittstelle falsch ist

Wenn mit `ndsconfig new` oder `ndsmanage` eine zweite Instanz des Verzeichnisses erstellt wird und die angegebene Schnittstelle falsch ist, versucht nds, die Standardschnittstelle zu verwenden. Wenn Sie einen nicht standardmäßigen Port angeben (beispielsweise 1524), ist die angegebene Schnittstelle falsch und es wird die Standardschnittstelle mit dem Port 524 verwendet.

Wenn die angegebene Schnittstelle für `n4u.server.interfaces` falsch ist, versucht `ndsd`, auf der ersten Schnittstelle zu überwachen. Die Portnummer wäre die in `n4u.server.tcp-port` angegebene Portnummer.

2.4.4 Neuaufbau des Verzeichnisses „.edir“

Das Verzeichnis `.edir` wird zur Verfolgung mehrere Instanzen von eDirectory verwendet. Um die verlorene oder beschädigte Instanzendatei neu zu erstellen (Datei `instances.$uid`, wobei `$uid` die Benutzer-ID des Benutzers im System darstellt), müssen die einzelnen Instanzendateien erstellt werden.

Die Dateien müssen den absoluten Standort der `nds.conf`-Dateien aller vom Benutzer konfigurierten Instanzen enthalten. Ein Benutzer mit der `uid` „1000“ muss beispielsweise die Instanzendatei `/etc/opt/novell/eDirectory/conf/.edir/instances.1000` mit den folgenden Einträgen erstellen:

```
/home/user1/instance1/nds.conf

/home/user1/instance2/nds.conf
```

3 Bestimmen der eDirectory-Versionsnummer

Die folgenden Abschnitte beschreiben, wie die auf einem Server installierte Version von eDirectory ermittelt werden kann:

- Abschnitt 3.1, „Windows“, auf Seite 23
- Abschnitt 3.2, „Linux“, auf Seite 24

3.1 Windows

- Führen Sie iMonitor aus.

  Klicken Sie auf der Seite „Agentenzusammenfassung“ auf „Bekannte Server“. Klicken Sie dann unter „Der Datenbank bekannte Server“ auf „Bekannte Server“. In der Spalte „Agentenrevision“ wird für jeden Server die interne Build-Nummer angezeigt. Die Agentenrevisionsnummer für eDirectory 8.7.1 kann beispielsweise „10510.64“ sein.

  Informationen zum Ausführen von iMonitor finden Sie unter „Zugreifen auf iMonitor“ im *NetIQ eDirectory 8.8 SP8-Administrationshandbuch*.
- Führen Sie `NDSCons.exe` aus.

  Doppelklicken Sie in der Windows-Systemsteuerung auf „NetIQ eDirectory Services“. Wählen Sie in der Spalte „Services“ den Eintrag „ds.dlm“ aus und klicken Sie auf „Konfigurieren“. Auf der Registerkarte „Agent“ werden sowohl die Marketingbezeichnung (zum Beispiel „NetIQ eDirectory 8.8.1) als auch die interne Build-Nummer (zum Beispiel „10510.64“) angezeigt.
- Führen Sie ein eDirectory-Dienstprogramm aus.

  Die meisten eDirectory-Dienstprogramme verfügen im Hilfemenü über die Option „Info“, die die Versionsnummer des Dienstprogramms anzeigt (zum Beispiel „Merge Graft Utility 10510.35“). Einige Dienstprogramme enthalten die interne Build-Nummer in ihrer Bezeichnung (zum Beispiel „DSRepair - Version 10510.37“).

  Um ein eDirectory-Dienstprogramm zu laden (beispielsweise DSMerge oder DSRepair), doppelklicken Sie in der Windows-Systemsteuerung auf „NetIQ eDirectory Services“. Wählen Sie in der Spalte „Services“ das Dienstprogramm aus und klicken Sie auf „Starten“.
- Zeigen Sie die Eigenschaften einer `.dlm`-Datei in eDirectory an.

  Klicken Sie im Windows Explorer mit der rechten Maustaste auf die Datei `.dlm` und klicken Sie dann im Dialogfeld „Eigenschaften“ auf die Registerkarte „Version“. Durch diese Aktion wird die Versionsnummer des Dienstprogramms angezeigt. Der Standardspeicherort für `.dlm`-Dateien in eDirectory ist `C:\novell\NDS`.

3.2 Linux

- Führen Sie „ndsstat“ aus.

  Das Dienstprogramm „ndsstat“ zeigt Informationen in Bezug auf die eDirectory-Server an, wie den eDirectory-Baumnamen, den vollständig qualifizierten Servernamen und die eDirectory-Version. Im folgenden Beispiel ist eDirectory 8.7.1 die Produktversion (Marketingbezeichnung) und 10510.65 die Binärversion (interne Build-Nummer).

  ```
  osg-dt-srv17:/>ndsstat
  Tree Name: SNMP-HPUX-RASH
  Server Name: .CN=osg-dt-srv17.O=novell.T=SNMP-HPUX-RASH.
  Binary Version: 10510.65
  Root Most Entry Depth: 0
  Product Version: NDS/Linux - NDS eDirectory v8.8.8 [DS]
  ```

  Informationen über das Ausführen von „ndsstat“ finden Sie unter „Linux-Befehle und Ihre Verwendung mit NetIQ eDirectory“ im *NetIQ eDirectory 8.8 SP8-Administrationshandbuch* und auf der man-Seite von ndsstat (`ndsstat.1m`).

- Führen Sie `ndsd --version` aus.

  Informationen über das Ausführen von „ndsd“ finden Sie unter „Linux-Befehle und Ihre Verwendung mit NetIQ eDirectory“ im *NetIQ eDirectory 8.8 SP8-Administrationshandbuch* und auf der man-Seite von ndsd (`ndsd.1m`).

- Führen Sie iMonitor aus.

  Klicken Sie auf der Seite „Agentenzusammenfassung“ auf „Bekannte Server“. Klicken Sie dann unter „Der Datenbank bekannte Server“ auf „Bekannte Server“. In der Spalte „Agentenrevision“ wird für jeden Server die interne Build-Nummer angezeigt. Die Agentenrevisionsnummer für NetIQ eDirectory 8.8.1 kann beispielsweise „10510.64“ sein.

  Informationen zum Ausführen von iMonitor finden Sie unter „Zugreifen auf iMonitor“ im *NetIQ eDirectory 8.8 SP8-Administrationshandbuch*.

- Führen Sie `rpm -qi NDSserv` aus.

  Nach der Eingabe dieses Befehls werden ähnliche Informationen wie bei `ndsd --version` angezeigt.

4 Protokolldateien

Dieser Abschnitt enthält Informationen zu den folgenden Protokolldateien:

4.1 modschema.log

Die Datei `modschema.log` enthält die Ergebnisse aller Schemaerweiterungen, die bei der Installation eines eDirectory-Servers in einem vorhandenen Baum vorgenommen wurden. In jeder Zeile des Protokolls werden die hinzugefügten bzw. geänderten Klassen und Attribute sowie der Status des Bearbeitungsversuchs angegeben.

Dieses Protokoll wird bei jeder Installation erstellt oder überschrieben, sodass es nur die Ergebnisse des letzten Installationsversuchs enthält. Zusätzlich zu den eDirectory-Schemaerweiterungen enthält dieses Protokoll die Ergebnisse aller weiteren Schemaerweiterungen, wie Lightweight Directory Access Protocol (LDAP) oder SAS, die vor dem Hinzufügen des neuen eDirectory-Servers von der Front-End-Anwendung DSINSTALL angewendet wurden.

Das Protokoll wird nicht generiert, wenn ein eigenständiger Server installiert wird oder die eDirectory-Version des Zielservers 7.0.1 oder höher ist.

4.2 dsinstall.log

Der erste Teil der Datei `dsinstall.log` enthält eine Liste der festgelegten Umgebungsvariablen. Der zweite Teil besteht aus Statusmeldungen, die den eDirectory-Installationsprozess dokumentieren.

4.3 ndsd.log

Die Datei `ndsd.log` enthält Informationen zu Meldungen in Bezug auf den eDirectory-Server, beispielsweise Meldungen über das Herunterfahren oder Starten des Servers oder der PKI- und LDAP-Services. Standardmäßig befindet sich diese Datei im Verzeichnis `/var/opt/novell/eDirectory/log`.

Sie können den Detailgrad der Datei `ndsd.log` erhöhen, indem Sie in der Datei `nds.conf` im Pfad `/etc/opt/novell/eDirectory/conf/nds.conf` die folgende Variable ändern:

```
n4u.server.log-levels=Logxxxx
```

Weitere Informationen zu den ndsd-Protokollierungsebenen finden Sie unter „Verwalten der Fehlerprotokollierung in eDirectory 8.8“ im *Handbuch zu den neuen Funktionen von NetIQ eDirectory 8.8 SP8*.

4.4 Festlegen der Protokolldateigröße unter Linux

Mit dem Parameter `n4u.server.log-file-size` in der Datei `nds.conf` können Sie die Größe der Protokolldatei festlegen. Die maximale Dateigröße beträgt 2 GB; die standardmäßige Dateigröße 1 MB. Sie können jedoch auch eine Dateigröße unter 1 MB festlegen.

Diese Einstellung wird nicht auf die Datei `ndsd.log` angewendet.

Wenn die Protokolldateigröße den angegebenen Grenzwert erreicht, wird die Protokolldatei beginnend vom Dateianfang überschrieben.

5 Problemsuche in LDIF-Dateien

Mit dem NetIQ Import Conversion Export (ICE)-Dienstprogramm können Sie auf einfache Weise LDIF-Dateien in eDirectory importieren und von eDirectory exportieren. Weitere Informationen finden Sie unter „NetIQ Import Conversion Export-Dienstprogramm“ im *NetIQ eDirectory 8.8 SP8-Administrationshandbuch*.

Für das ordnungsgemäße Funktionieren eines LDIF-Imports benötigen Sie zunächst eine LDIF-Datei, die das NetIQ Import Conversion Export-Dienstprogramm lesen und verarbeiten kann. Dieser Abschnitt behandelt das LDIF-Dateiformat und die LDIF-Syntax und liefert Beispiele für korrekte LDIF-Dateien.

5.1 Funktionsweise von LDIF

LDIF ist ein weit verbreitetes Dateiformat, das Directory-Informationen oder Änderungsoperationen beschreibt, die für ein Directory ausgeführt werden können. LDIF ist vollständig unabhängig vom Speicherformat, das für eine bestimmte Directory-Implementierung verwendet wird, und wird gewöhnlich zum Exportieren von Directory-Informationen von und zum Importieren von Daten nach LDAP-Servern verwendet.

LDIF ist üblicherweise einfach zu erstellen. Dies ermöglicht die Verwendung von Werkzeugen wie awk oder perl, um Daten von einem systemeigenen Format in ein LDAP-Directory zu verschieben. Darüber hinaus können Sie Skripten erstellen, um Testdaten im LDIF-Format zu erstellen.

5.1.1 LDIF-Dateiformat

Für den Import mit dem NetIQ Import Conversion Export-Dienstprogramm sind LDIF 1-formatierte Dateien erforderlich. Folgende Grundregeln gelten für LDIF 1-Dateien:

- Die erste Zeile, die kein Kommentar ist, muss „version: 1“ lauten.
- Auf die Version folgen eine oder mehrere Datensätze.
- Jeder Datensatz besteht aus Feldern, wobei pro Zeile ein Feld vorhanden ist.
- Die Zeilen werden durch einen Zeilenvorschub oder eine Kombination aus Zeilenumschaltung/ Zeilenvorschub getrennt.
- Datensätze werden durch eine oder mehrere Leerzeilen getrennt.

- Es gibt zwei verschiedene Arten von LDIF-Datensätzen: Inhaltsdatensätze und Änderungsdatensätze. Eine LDIF-Datei kann eine unbegrenzte Anzahl von Datensätzen enthalten, sie müssen jedoch alle den gleichen Typ aufweisen. Es ist nicht möglich, Inhaltsdatensätze und Änderungsdatensätze in einer LDIF-Datei zu mischen.
- Jede Zeile, die mit dem Nummernzeichen (#) beginnt, ist ein Kommentar und wird bei der Verarbeitung der LDIF-Datei ignoriert.

5.1.2 LDIF-Inhaltsdatensätze

Ein LDIF-Inhaltsdatensatz repräsentiert die Inhalte eines vollständigen Eintrags. Es folgt ein Beispiel für eine LDIF-Datei mit vier Inhaltsdatensätzen:

```
 1  version: 1
 2  dn: c=US
 3  objectClass: top
 4  objectClass: country
 5
 6  dn: l=San Francisco, c=US
 7  objectClass: top
 8  objectClass: locality
 9  st: San Francisco
10
11 dn: ou=Artists, l=San Francisco, c=US
12 objectClass: top
13 objectClass: organizationalUnit
14 telephoneNumber: +1 415 555 0000
15
16 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US
17 sn: Michaels
18 givenname: Peter
19 objectClass: top
20 objectClass: person
21 objectClass: organizationalPerson
22 objectClass: iNetOrgPerson
23 telephonenumber: +1 415 555 0001
24 mail: Peter.Michaels@aaa.com
25 userpassword: Peter123
26
```

Diese LDIF-Datei besteht aus den folgenden Bestandteilen:

Komponente	Beschreibung
Versionsbezeichner	Die erste Zeile einer LDIF-Datei enthält die Version. Null oder mehr Zeilen sind zwischen dem Doppelpunkt und der Versionsnummer zulässig, die derzeit als "1" definiert ist. Falls die Versionszeile fehlt, kann jede Anwendung, welche die LDIF-Datei verarbeitet, von der Version 0 für die Datei ausgehen. Es ist außerdem möglich, dass die LDIF-Datei als syntaktisch falsch abgelehnt wird. Dienstprogramme von NetIQ, die LDIF verarbeiten, gehen von der Dateiversion 0 aus, wenn die Versionszeile fehlt.

Komponente	Beschreibung
Bezeichner für den eindeutigen Namen	Die erste Zeile jedes Inhaltsdatensatzes (die Zeilen 2, 6, 11 und 16 im obigen Beispiel) bezeichnet den eindeutigen Namen (DN) des repräsentierten Eintrags. Der DN-Bezeichner muss eines der folgenden beiden Formate aufweisen: ◆ dn: *safe_UTF-8_distinguished_name* ◆ dn:: *Base64_encoded_distinguished_name*
Zeilenbegrenzungszeichen	Das Zeilentrennzeichen kann ein Zeilenvorschub oder eine Kombination aus Zeilenumschaltung/Zeilenvorschub darstellen. Dies behebt eine allgemeine Inkompatibilität zwischen Linux- und Solaris-Textdateien, die einen Zeilenvorschub als Zeilentrennzeichen verwenden, und MS-DOS*- und Windows-Textdateien, die eine Kombination aus Zeilenumschaltung/ Zeilenvorschub als Zeilentrennzeichen verwenden.
Datensatzbegrenzungszeichen	Leerzeilen (die Zeilen 5, 10, 15 und 26 im obigen Beispiel) werden als Datensatzbegrenzungszeichen verwendet. Jeder Datensatz in einer LDIF-Datei, einschließlich des letzten Datensatzes, muss mit einem Datensatzbegrenzungszeichen beendet werden (eine oder mehrere Leerzeilen). Zwar akzeptieren einige Implementierungen eine LDIF-Datei ohne abschließendes Datensatzbegrenzungszeichen, aber für die LDIF-Spezifikation ist dies erforderlich.
Attributwertbezeichner	Alle anderen Zeilen in einem Inhaltsdatensatz sind Wertbezeichner. Wertbezeichner müssen eines der folgenden drei Formate aufweisen: ◆ Attribute description: *Wert* ◆ Attribute description:: *Base64_kodierter_Wert* ◆ Attribute description: < *URL*

5.1.3 LDIF-Änderungsdatensätze

LDIF-Änderungsdatensätze enthalten Änderungen, die an einem Directory vorgenommen werden sollen. Jede LDAP-Aktualisierungsoperation (Hinzufügen, Löschen, Ändern und DN ändern) können in einem LDIF-Änderungsdatensatz dargestellt werden.

LDIF-Änderungsdatensätze verwenden dasselbe Format für den Bezeichner des eindeutigen Namens, den Attributwertbezeichner und das Datensatzbegrenzungszeichen wie LDIF-Inhaltsdatensätze. (Weitere Informationen hierzu finden Sie unter „LDIF-Inhaltsdatensätze“, auf Seite 28.) Das Vorhandensein eines `changetype`-Felds unterscheidet einen LDIF-Änderungsdatensatz von einem LDIF-Inhaltsdatensatz. Ein `changetype`-Feld identifiziert die durch den Änderungsdatensatz angegebene Operation.

Für ein `changetype`-Feld sind die folgenden fünf Formate möglich:

Formular	Beschreibung
changetype:add	Ein Schlüsselwort, das für den Änderungsdatensatz eine LDAP-Operation zum Hinzufügen festlegt.

Formular	Beschreibung
changetype:delete	Ein Schlüsselwort, das für den Änderungsdatensatz eine LDAP-Operation zum Löschen festlegt.
changetype: moddn	Ein Schlüsselwort, das für den Änderungsdatensatz eine LDAP-Operation zum Ändern des DN festlegt, falls der LDIF-Prozessor an den LDAP-Server als Version 3-Client gebunden ist, oder eine Operation zum Ändern des RDN, falls der LDIF-Prozessor an den LDAP-Server als Version 2-Client gebunden ist.
changetype: modrdn	Ein Synonym für den moddn-Änderungstyp.
changetype:modify	Ein Schlüsselwort, das für den Änderungsdatensatz eine LDAP-Operation zum Ändern festlegt.

Der Änderungstyp "Add"

Ein Änderungsdatensatz vom Typ „Add“ (Hinzufügen) ähnelt einem Inhaltsänderungsdatensatz (siehe „LDIF-Inhaltsdatensätze“, auf Seite 28), verfügt jedoch genau vor den Attributwertfeldern zusätzlich über das Feld „changetype: add“.

Alle Datensätze müssen den gleichen Typ aufweisen. Es ist nicht möglich, Inhalts- und Änderungsdatensätze zu mischen.

```
 1 version: 1
 2 dn: c=US
 3 changetype: add
 4 objectClass: top
 5 objectClass: country
 6
 7 dn: l=San Francisco, c=US
 8 changetype: add
 9 objectClass: top
10 objectClass: locality
11 st: San Francisco
12
14 dn: ou=Artists, l=San Francisco, c=US
15   changetype: add
16 objectClass: top
17 objectClass: organizationalUnit
18 telephoneNumber: +1 415 555 0000
19
20 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US
21 changetype: add
22 sn: Michaels
23 givenname: Peter
24 objectClass: top
25 objectClass: person
26 objectClass: organizationalPerson
27 objectClass: iNetOrgPerson
28 telephonenumber: +1 415 555 0001
29 mail: Peter.Michaels@aaa.com
30 userpassword: Peter123
31
```

Der Änderungstyp "Delete"

Ein delete-Änderungsdatensatz bezeichnet das Löschen eines Eintrags, weshalb für einen delete-Änderungsdatensatz nur die Felder für den Bezeichner des eindeutigen Namens und der delete-Änderungstyp erforderlich sind.

Es folgt ein Beispiel für eine LDIF-Datei, mit der die vier Einträge gelöscht werden, die erstellt wurden von der LDIF-Datei im Abschnitt „Der Änderungstyp "Add"“, auf Seite 30.

WICHTIG: Um Einträge zu löschen, die Sie zuvor hinzugefügt haben, kehren Sie die Reihenfolge der Einträge um. Wenn dies nicht erfolgt, tritt beim Löschvorgang ein Fehler auf, weil die Containereinträge nicht leer sind.

```
 1 version: 1
 2 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US
 3 changetype: delete
 4
 5 dn: ou=Artists, l=San Francisco, c=US
 8   changetype: delete
 9
10 dn: l=San Francisco, c=US
11 changetype: delete
12
13 dn: c=US
14 changetype: delete
15
```

Der Änderungstyp "Modify"

Mit dem modify-Änderungstyp legen Sie das Hinzufügen, Löschen und Ersetzen von Attributwerten für einen bereits vorhandenen Eintrag fest. Änderungen weisen eines der folgenden drei Formate auf:

Element	Beschreibung
add: Attributtyp	Ein Schlüsselwort, das angibt, dass nachfolgende Attributwertbezeichner für den Attributtyp zum Eintrag hinzugefügt werden sollen.
delete: Attributtyp	Ein Schlüsselwort, das angibt, dass Werte des Attributtyps gelöscht werden sollen. Wenn Attributwertbezeichner auf das delete-Feld folgen, werden die angegebenen Werte gelöscht. Wenn keine Attributwertbezeichner auf das delete-Feld folgen, werden alle Werte gelöscht. Weist das Attribut keine Werte auf, schlägt diese Operation fehl, aber der gewünschte Effekt wird dennoch erzielt, weil für das Attribut keine zu löschenden Werte vorhanden waren.
replace: Attributtyp	Ein Schlüsselwort, das angibt, dass Werte des Attributtyps ersetzt werden sollen. Alle Attributwertbezeichner, die auf das replace-Feld folgen, werden zu den neuen Werten für den Attributtyp. Wenn keine Attributwertbezeichner auf das replace-Feld folgen, werden die aktuellen Werte durch leere Werte ersetzt (wodurch das Attribut gelöscht wird). Im Gegensatz zum delete-Änderungsbezeichner wird die Ersetzung dennoch erfolgreich ausgeführt, wenn das Attribut keine Werte aufweist. Das Endergebnis ist in beiden Fällen identisch.

Im nachfolgenden Beispiel für einen modify-Änderungstyp wird zum Eintrag `cn=Peter Michaels` eine zusätzliche Telefonnummer hinzugefügt.

```
 1 version: 1
 2 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US
 3 changetype: modify
 4 # add the telephone number to cn=Peter Michaels
 4 add: telephonenumber
 5 telephonenumber: +1 415 555 0002
 6
```

So wie mehrere Änderungen in einer einzigen LDAP-Änderungsanforderung kombiniert werden können, können Sie mehrere Änderungen in einem einzigen LDIF-Datensatz angeben. Mit einer Zeile, die nur einen Bindestrich (-) aufweist, wird das Ende der Attributwertspezifikationen für jeden Änderungsbezeichner markiert.

Die folgende LDIF-Beispieldatei enthält verschiedene Änderungen:

```
 1 version: 1
 2
 3 # An empty line to demonstrate that one or more
 4 # line separators between the version identifier
 5 # and the first record is legal.
 6
 7 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US
 8 changetype: modify
 9 # Add an additional telephone number value.
10 add: telephonenumber
11 telephonenumber: +1 415 555 0002
12 -
13 # Delete the entire fascimiletelephonenumber attribute.
14 delete: facsimileTelephoneNumber
15 -
16 # Replace the existing description (if any exists)
17 # with two new values.
18 replace: description
19 description: guitar player
20 description: solo performer
21 -
22 # Delete a specific value from the telephonenumber
23 # attribute.
24 delete: telephonenumber
25 telephonenumber: +1 415 555 0001
26 -
27 # Replace the existing title attribute with an empty
28 # set of values, thereby causing the title attribute to
29 # be removed.
30 replace: title
31 -
32
```

Der Änderungstyp "Modify DN"

Mit dem Änderungstyp "modify DN" können Sie einen Eintrag umbenennen, verschieben, oder beides. Dieser Änderungstyp besteht aus zwei erforderlichen Feldern und einem optionalen Feld.

Feld	Beschreibung
newrdn (erforderlich)	Liefert den neuen Namen für den Eintrag, der beim Verarbeiten dieses Datensatzes zugewiesen wird. Der newrdn-Bezeichner muss eines der folgenden beiden Formate aufweisen: ◆ newrdn: *safe_UTF-8_relativer_eindeutiger_Name* ◆ newrdn:: *Base64_kodierter_relativer_eindeutiger_Name* Der newrdn-Bezeichner ist in allen LDIF-Datensätzen des Änderungstyps "modify DN" erforderlich.
deleteoldrdn (erforderlich)	Der deleteoldrdn-Bezeichner ist eine Flagge, die anzeigt, ob der alte RDN durch den "newrdn" ersetzt werden oder aber beibehalten werden soll. Dieser Bezeichner weist eines der folgenden Formate auf: ◆ deleteoldrdn: 0 Der alte RDN-Wert sollte nach dem Umbenennen des Eintrags in diesem erhalten bleiben. ◆ deleteoldrdn: 1 Der alte RDN-Wert sollte nach dem Umbenennen des Eintrags gelöscht werden.
newsuperior (optional)	Der newsuperior-Bezeichner liefert den Namen des neuen übergeordneten Objekts, der beim Verarbeiten des "modify DN"-Datensatzes dem Eintrag zugewiesen wird. Der newsuperior-Bezeichner muss eines der folgenden beiden Formate aufweisen: ◆ newsuperior: *safe_UTF-8_eindeutiger_Name* ◆ newsuperior:: *Base64_kodierter_eindeutiger_Name* Der newsuperior-Bezeichner ist in LDIF-Datensätzen des Änderungstyps "modify DN" optional. Er wird nur verwendet, wenn Sie dem Eintrag ein neues übergeordnetes Objekt zuweisen möchten.

Es folgt ein Beispiel für den Änderungstyp „modify DN“, das veranschaulicht, wie ein Eintrag umbenannt wird:

```
1 version: 1
2
3 # Rename ou=Artists to ou=West Coast Artists, and leave
4 # its old RDN value.
5 dn: ou=Artists,l=San Francisco,c=US
6 changetype: moddn
7 newrdn: ou=West Coast Artists
8 deleteoldrdn: 1
9
```

Es folgt ein Beispiel für den Änderungstyp „modify DN“, das veranschaulicht, wie ein Eintrag verschoben wird:

```
 1 version: 1
 2
 3 # Move cn=Peter Michaels from
 4 # ou=Artists,l=San Francisco,c=US to
 5 # ou=Promotion,l=New York,c=US and delete the old RDN.
 5 dn: cn=Peter Michaels,ou=Artists,l=San Francisco,c=US
 6 changetype: moddn
 7 newrdn: cn=Peter Michaels
 8 deleteoldrdn: 1
 9 newsuperior: ou=Promotion,l=New York,c=US
10
```

Es folgt ein Beispiel für den Änderungstyp „modify DN", das veranschaulicht, wie ein Eintrag gleichzeitig verschoben und umbenannt wird:

```
 1 version: 1
 2
 3 # Move ou=Promotion from l=New York,c=US to
 4 # l=San Francisco,c=US and rename it to
 5 # ou=National Promotion.
 5 dn: ou=Promotion,l=New York,c=US
 6 changetype: moddn
 7 newrdn: ou=National Promotion
 8 deleteoldrdn: 1
 9 newsuperior: l=San Francisco,c=US
10
```

WICHTIG: Die RDN-Änderungsoption von LDAP 2 unterstützt das Verschieben von Einträgen nicht. Wenn Sie versuchen, einen Eintrag über die LDIF-Syntax `newsuperior` mit einem LDAP 2-Client zu verschieben, tritt ein Fehler bei der Anforderung auf.

5.1.4 Zeilenumbruch in LDIF-Dateien

Um eine Zeile in einer LDIF-Datei umzubrechen, fügen Sie einfach ein Zeilentrennzeichen (einen Zeilenvorschub oder eine Kombination aus Zeilenumschaltung/Zeilenvorschub) gefolgt von einem Leerzeichen an der Stelle ein, an der die Zeile umgebrochen werden soll. Wenn die LDIF-Analyse ein Leerzeichen am Beginn der Zeile findet, bedeutet dies, dass die restlichen Daten in der Zeile mit den Daten in der vorherigen Zeile verkettet werden müssen. Das vorangestellte Leerzeichen wird dann verworfen.

Sie sollten Zeilen nicht in der Mitte eines aus mehreren Byte bestehenden UTF-8-Zeichens umbrechen.

Es folgt ein Beispiel für eine LDIF-Datei mit einer umgebrochenen Zeile (siehe Zeile 13 und 14):

```
 1 version: 1
 2 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US
 3 sn: Michaels
 4 givenname: Peter
 5 objectClass: top
 6 objectClass: person
 7 objectClass: organizationalPerson
 8 objectClass: iNetOrgPerson
 9 telephonenumber: +1 415 555 0001
10 mail: Peter.Michaels@aaa.com
11 userpassword: Peter123
12 description: Peter is one of the most popular music
13  ians recording on our label. He’s a big concert dr
14  aw, and his fans adore him.
15
```

5.1.5 Darstellung von Passwörtern mit Hash in LDIF-Dateien

Passwörter mit Hash werden in der LDIF-Datei als base64-Daten dargestellt. Nach dem Attributnamen `userpassword` muss die Bezeichnung der für das Hashing des Passworts verwendeten Verschlüsselung angegeben werden. Diese Bezeichnung muss in geschweifte Klammern „{ }" gesetzt werden, wie im folgenden Beispiel dargestellt:

Beispiel 1

Für Passwörter mit SHA-Hashing:

```
1 version: 1 2 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US 3 sn:
Michaels 4 userpassword: {SHA}xcbdh46ngh37jsd0naSFDedjAS30dm5 objectclass:
inetOrgPerson
```

Beispiel 2

Für Passwörter mit SSHA-Hashing:

```
1 version: 1 2 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US 3 sn:
Michaels 4 userpassword: {SSHA}sGs948DFGkakdfkasdDF34DF4dS3skl5DFS5 objectclass:
inetOrgPerson
```

Beispiel 3

Für Passwörter mit MD5-Hashing:

```
1 version: 1 2 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US 3 sn:
Michaels 4 userpassword: {MD5}a45lkSDF234SDFG62dsfsf2DG2QEvgdmnk4305 objectclass:
inetOrgPerson
```

5.2 Fehlerbehebung in LDIF-Dateien

- „Vorverweise aktivieren", auf Seite 35
- „Syntax von LDIF-Dateien überprüfen", auf Seite 38
- „LDIF-Fehlerdatei verwenden", auf Seite 39
- „LDAP-SDK-Flaggen für die Fehlersuche verwenden", auf Seite 40

Berücksichtigen Sie die folgenden Abschnitte, falls bei einer LDIF-Datei Probleme auftreten:

5.2.1 Vorverweise aktivieren

Es kann hin und wieder vorkommen, dass Sie auf LDIF-Dateien stoßen, in denen ein Datensatz zum Hinzufügen eines Eintrags vor einem Datensatz zum Hinzufügen seines übergeordneten Objekts angeordnet ist. In diesem Fall wird ein Fehler gemeldet, weil das übergeordnete Objekt des neuen Eintrags nicht vorhanden ist, wenn der LDAP-Server versucht, den Eintrag hinzuzufügen.

Um dieses Problem zu beheben, aktivieren Sie einfach die Verwendung von Vorverweisen. Wenn Sie das Erstellen von Vorverweisen aktivieren und ein Eintrag erstellt wird, bevor das übergeordnete Objekt existiert, wird ein Platzhalter, ein so genannter Vorverweis, für das übergeordnete Objekt des Eintrags erstellt, damit der Eintrag erfolgreich erstellt werden kann. Wird das übergeordnete Objekt später erstellt, wird der Vorverweis in einen normalen Eintrag geändert.

Es besteht die Möglichkeit, dass Vorverweise nach Abschluss des LDIF-Imports erhalten bleiben (z. B. wenn die LDIF-Datei niemals das übergeordnete Objekt für einen Eintrag erstellt hat). In diesem Fall wird der Vorverweis in ConsoleOne und iManager als unbekanntes Objekt angezeigt. Sie können zwar nach einem Vorverweiseintrag suchen, aber keine Attribute (außer "objectClass") im Vorverweiseintrag lesen, weil er keine Attribute oder Attributwerte aufweist. Alle LDAP-Operationen funktionieren jedoch für die Objekteinträge, die sich unterhalb des Vorverweises befinden, wie gewohnt.

Vorverweiseinträge identifizieren

Vorverweiseinträge haben die Objektklasse "Unbekannt", und ihre interne Eintragsflagge NDS EF_REFERENCE ist gesetzt. In ConsoleOne und iManager werden Einträge mit der Objektklasse „Unbekannt“ durch ein rundes gelbes Symbol mit einem Fragezeichen in der Mitte dargestellt. Sie können LDAP verwenden, um Objekte mit der Objektklasse "Unbekannt" zu suchen. Es gibt jedoch zur Zeit keine Möglichkeit, um mit LDAP mit Sicherheit festzustellen, dass es sich bei den Eintragsflaggeneinstellungen um Vorverweiseinträge handelt.

Vorverweiseinträge in normale Objekte ändern

Sie können einen Vorverweiseintrag in ein normales Objekt ändern, indem Sie es einfach erstellen (z.B. mithilfe einer LDIF-Datei- oder einer LDAP-Clientanforderung). Wenn Sie eDirectory auffordern, einen Eintrag zu erstellen, der als Vorverweis existiert, wandelt eDirectory den vorhandenen Vorverweiseintrag in das gewünschte Objekt um.

Arbeiten mit dem NetIQ eDirectory-Assistenten für Import, Konvertierung und Export

So aktivieren Sie Vorverweise während eines LDIF-Imports:

1. Klicken Sie in NetIQ iManager auf die Schaltfläche *Rollen und Aufgaben* .
2. Klicken Sie auf *eDirectory-Wartung* > *Assistent für Import, Konvertierung und Export*.
3. Klicken Sie auf *Daten aus einer Datei* > *auf dem Datenträger importieren* und dann auf *Weiter*.
4. Wählen Sie *LDIF* als zu importierenden Dateityp aus.
5. Geben Sie den Namen der Datei an, die die zu importierenden Daten enthält, legen Sie die geeigneten Optionen fest und klicken Sie dann auf *Weiter*.
6. Geben Sie den LDAP-Server an, auf dem die Daten importiert werden sollen.
7. Fügen Sie wie in nachfolgender Tabelle beschrieben die entsprechenden Optionen hinzu:

Option	Beschreibung
Server-DNS-Name/IP-Adresse	DNS-Name oder IP-Adresse des LDAP-Zielservers
Anschluss	Ganzzahlige Anschlussnummer des LDAP-Zielservers
DER-Datei	Name der DER-Datei, die einen Serverschlüssel für die SSL-Authentifizierung enthält
Anmeldemethode	Authentifizierte Anmeldung oder anonyme Anmeldung (für den im Feld „Benutzer-DN“ angegebenen Eintrag)
Benutzer-DN	Eindeutiger Name des Eintrags, der beim Binden mit der vom Server angegebenen Bindeoperation verwendet werden soll
Passwort	Passwortattribut des Eintrags im Feld „Benutzer-DN“

8. Klicken Sie unter *Erweiterte Einstellungen* auf *Vorverweise zulassen*.
9. Klicken Sie auf *Weiter* und dann auf *Fertig stellen*.

So aktivieren Sie Vorverweise während einer Migration von Daten zwischen Servern:

1. Klicken Sie in NetIQ iManager auf die Schaltfläche *Rollen und Aufgaben* .
2. Klicken Sie auf *eDirectory-Wartung* > *Assistent für Import, Konvertierung und Export*.
3. Klicken Sie auf *Daten zwischen den Servern migrieren* und dann auf *Weiter*.
4. Geben Sie den LDAP-Server an, auf dem die Einträge vorhanden sind, die Sie migrieren möchten.
5. Fügen Sie wie in nachfolgender Tabelle beschrieben die entsprechenden Optionen hinzu:

Option	Beschreibung
Server-DNS-Name/IP-Adresse	DNS-Name oder IP-Adresse des LDAP-Ursprungsservers
Anschluss	Ganzzahlige Anschlussnummer des LDAP-Ursprungsservers
DER-Datei	Name der DER-Datei, die einen Serverschlüssel für die SSL-Authentifizierung enthält
Anmeldemethode	Authentifizierte Anmeldung oder anonyme Anmeldung (für den im Feld „Benutzer-DN“ angegebenen Eintrag)
Benutzer-DN	Eindeutiger Name des Eintrags, der beim Binden mit der vom Server angegebenen Bindeoperation verwendet werden soll
Passwort	Passwortattribut des Eintrags im Feld „Benutzer-DN“

6. Klicken Sie unter *Erweiterte Einstellungen* auf *Vorverweise zulassen*.
7. Klicken Sie auf *Weiter*.
8. Geben Sie die Suchkriterien (unten beschrieben) für die Einträge ein, die Sie migrieren möchten:

Option	Beschreibung
Basis-DN	Eindeutiger Basisname für die Suchanforderung Falls dieses Feld leer ist, wird als Basis-DN "" (leere Zeichenkette) voreingestellt.
Bereich	Bereich der Suchanforderung
Filter	RFC-2254-kompatibler Suchfilter Der Standardwert ist `objectclass=*`.
Attribute	Attribute, die für jeden Sucheintrag zurückgegeben werden sollen

9. Klicken Sie auf *Weiter*.
10. Geben Sie den LDAP-Server an, auf den die Daten migriert werden sollen.
11. Klicken Sie auf *Weiter* und dann auf *Fertig stellen*.

HINWEIS: Stellen Sie sicher, dass das Schema für alle LDAP-Services konsistent ist.

Befehlszeilenschnittstelle des NetIQ Import Conversion Export-Dienstprogramms

Um Vorverweise in der Befehlszeilenschnittstelle zu aktivieren, verwenden Sie die Option -F der LDAP-Zielbehandlungsroutine.

Weitere Informationen finden Sie unter „Optionen für die LDIF-Zielbehandlungsroutine“ im *NetIQ eDirectory 8.8 SP8-Administrationshandbuch*.

5.2.2 Syntax von LDIF-Dateien überprüfen

Die Syntax einer LDIF-Datei kann vor der Verarbeitung der Datensätze in der Datei überprüft werden. Sie verwenden dazu die Option „Vorgänge anzeigen, aber nicht durchführen“ der LDIF-Ursprungsbehandlungsroutine.

Die LDIF-Ursprungsbehandlungsroutine überprüft stets die Syntax der Datensätze in einer LDIF-Datei bei deren Verarbeitung. Mit dieser Option wird die Verarbeitung der Datensätze deaktiviert und ermöglicht Ihnen die Überprüfung der Syntax.

Arbeiten mit dem NetIQ eDirectory-Assistenten für Import, Konvertierung und Export

1. Klicken Sie in NetIQ iManager auf die Schaltfläche *Rollen und Aufgaben* .
2. Klicken Sie auf *eDirectory-Wartung* > *Assistent für Import, Konvertierung und Export*.
3. Klicken Sie auf *Daten aus einer Datei* > *auf dem Datenträger importieren* und dann auf *Weiter*.
4. Wählen Sie *LDIF* als zu importierenden Dateityp aus.
5. Geben Sie den Namen der Datei an, die die zu importierenden Daten enthält, und legen Sie die geeigneten Optionen fest.

6. Klicken Sie unter *Erweiterte Einstellungen* auf *Vorgänge anzeigen, aber nicht durchführen* und dann auf *Weiter*.
7. Geben Sie den LDAP-Server an, auf dem die Daten importiert werden sollen.
8. Fügen Sie wie in nachfolgender Tabelle beschrieben die entsprechenden Optionen hinzu:

Option	Beschreibung
Server-DNS-Name/IP-Adresse	DNS-Name oder IP-Adresse des LDAP-Zielservers
Anschluss	Ganzzahlige Anschlussnummer des LDAP-Zielservers
DER-Datei	Name der DER-Datei, die einen Serverschlüssel für die SSL-Authentifizierung enthält
Anmeldemethode	Authentifizierte Anmeldung oder anonyme Anmeldung (für den im Feld „Benutzer-DN“ angegebenen Eintrag)
Benutzer-DN	Eindeutiger Name des Eintrags, der beim Binden mit der vom Server angegebenen Bindeoperation verwendet werden soll
Passwort	Passwortattribut des Eintrags im Feld „Benutzer-DN“

9. Klicken Sie auf *Weiter* und dann auf *Fertig stellen*.

Befehlszeilenschnittstelle des NetIQ Import Conversion Export-Dienstprogramms

Um die Syntax einer LDIF-Datei mithilfe der Befehlszeilenschnittstelle zu überprüfen, verwenden Sie die Option -n der LDIF-Ursprungsbehandlungsroutine.

Weitere Informationen finden Sie unter „Optionen für die LDIF-Ursprungsbehandlungsroutine“ im NetIQ eDirectory 8.8 SP8-Administrationshandbuch.

5.2.3 LDIF-Fehlerdatei verwenden

Das NetIQ Import-/Umwandlungs-/Exportprogramm erstellt automatisch eine LDIF-Datei, in der alle Datensätze aufgeführt sind, die nicht durch die Zielbehandlungsroutine verarbeitet werden konnten. Sie können die von dem Dienstprogramm erstellte LDIF-Fehlerdatei bearbeiten, die Fehler beheben und dann erneut auf den Server anwenden, um einen Importvorgang oder eine Datenmigration abzuschließen, in dem bzw. der fehlerhafte Datensätze vorhanden waren.

Arbeiten mit dem NetIQ eDirectory-Assistenten für Import und Export

Diese Funktion ist nur in ConsoleOne verfügbar.

1. Klicken Sie in ConsoleOne auf *Assistent* > *NDS-Import/-Export*.
2. Klicken Sie auf die Aufgabe, die Sie ausführen möchten.
3. Klicken Sie auf *Erweitert*.
4. Geben Sie im Feld *Protokolldatei* den Namen einer Datei an, in der Ausgabemeldungen (einschließlich Fehlermeldungen) protokolliert werden.
5. Geben Sie im Feld *LDIF-Ausgabedatei für fehlerhafte Datensätze* den Namen einer Datei an, in der fehlerhafte Einträge im LDIF-Format ausgegeben werden.

Sie können diese Datei zur Prüfung und Behebung von Fehlern verwenden. Sie können auch eine bearbeitete (korrigierte) Version dieser Datei erneut auf das Verzeichnis anwenden.

6 Klicken Sie auf *Schließen*.

7 Befolgen Sie die Online-Anweisungen, um die gewählte Aufgabe zu beenden.

Befehlszeilenschnittstelle des NetIQ Import Conversion Export-Dienstprogramms

Um Fehlerprotokolloptionen im Befehlszeilenprogramm zu konfigurieren, verwenden Sie die allgemeine Option `-l`.

Weitere Informationen finden Sie unter „Allgemeine Optionen“ im NetIQ eDirectory 8.8 SP8-Administrationshandbuch.

5.2.4 LDAP-SDK-Flaggen für die Fehlersuche verwenden

Für das Verständnis bestimmter LDIF-Probleme sollten Sie wissen, wie das LDAP-Client-SDK funktioniert. Sie können die folgenden Flaggen zur Fehlersuche für die LDAP-Ursprungsbehandlungsroutine und/oder die LDAP-Zielbehandlungsroutine festlegen.

Wert	Beschreibung
0x0001	LDAP-Funktionsaufrufe verfolgen.
0x0002	Informationen über Pakete drucken.
0x0004	Informationen zu Argumenten drucken.
0x0008	Verbindungsinformationen drucken.
0x0010	Informationen zur BER-Verschlüsselung und –Entschlüsselung drucken.
0x0020	Informationen zu Suchfiltern drucken.
0x0040	Konfigurationsinformationen drucken.
0x0080	Informationen zu den Zugriffssteuerungslisten (ACLs) drucken.
0x0100	Statistische Informationen drucken.
0x0200	Zusätzliche statistische Informationen drucken.
0x0400	Shellinformationen drucken.
0x0800	Analyseinformationen drucken.
0xFFFF (-1 Decimal)	Alle Fehlersuchoptionen aktivieren.

Sie können diese Funktion mit der Option `-e` für die LDAP-Ziel- und LDAP-Ursprungsbehandlungsroutine aktivieren. Der ganzzahlige Wert, den Sie für die Option `-e` eingeben, ist eine Bitmaske, die verschiedene Arten von Fehlersuchinformationen im LDAP-SDK ermöglicht.

Weitere Informationen finden Sie unter „Optionen für die LDAP-Ursprungsbehandlungsroutine“ und „Optionen für die LDAP-Zielbehandlungsroutine“ im *NetIQ eDirectory 8.8 SP8-Administrationshandbuch*.

5.3 LDIF zum Erweitern des Schemas verwenden

LDIF kann LDAP-Aktualisierungsoperationen darstellen, weshalb Sie mit LDIF das Schema ändern können.

5.3.1 Neue Objektklasse hinzufügen

Zum Hinzufügen einer Klasse fügen Sie einfach einen Attributwert hinzu, welcher der Spezifikation für `NDSObjectClassDescription` für das Attribut `objectClasses` von `subschemaSubentry` entspricht.

```
NDSObjectClassDescription = "(" whsp
   numericoid whsp
   [ "NAME" qdescrs ]
   [ "DESC" qdstring ]
   [ "OBSOLETE" whsp ]
   [ "SUP" oids ]
   [ ( "ABSTRACT" / "STRUCTURAL" / "AUXILIARY" ) whsp ]
   [ "MUST" oids ]
   [ "MAY" oids ]
   [ "X-NDS_NOT_CONTAINER" qdstrings ]
   [ "X-NDS_NONREMOVABLE" qdstrings ]
   [ "X-NDS_CONTAINMENT" qdstrings ]
   [ "X-NDS_NAMING" qdstrings ]
   [ "X-NDS_NAME" qdstrings ]
   whsp ")"
```

Die folgende LDIF-Beispieldatei fügt die Objektklasse `person` zum Schema hinzu:

```
 1 version: 1
 2 dn: cn=schema
 3 changetype: add
 4 objectClasses: ( 2.5.6.6 NAME 'person' DESC 'Standard
 5   ObjectClass' SUP ndsLoginProperties STRUCTURAL MUST
 6   (cn $ sn) MAY (description $ seeAlso $ telephoneNum
 7  ber $ fullName $ givenName $ initials $ uid $ userPa
 8  ssword) X-NDS_NAMING ('cn' 'uid') X-NDS_CONTAINMENT
 9  ('organization' 'organizationalUnit' 'domain') X-NDS
10  _NAME 'Person' X-NDS_NOT_CONTAINER '1' X-NDS_NONREMO
11  VABLE '1')
12
```

Obligatorische Attribute

Obligatorische Attribute werden im `MUST`-Abschnitt der Objektklassenbeschreibung aufgeführt. Bei der Objektklasse „person“ lauten die obligatorischen Attribute `cn` und `sn`.

Optionale Attribute

Optionale Attribute werden im `MAY`-Abschnitt der Objektklassenbeschreibung aufgeführt. Die optionalen Attribute der Objektklasse `person` sind `description`, `seeAlso`, `telephoneNumber`, `fullName`, `givenName`, `initials`, `uid` und `userPassword`.

HINWEIS: Das Attribut `userPassword` darf nicht als optionales Attribut (im Abschnitt `MAY`) verwendet werden. Bei der Operation tritt ein Fehler auf, wenn Sie versuchen, das Attribut als obligatorisches Attribut (`MUST`) in der neuen `objectClass` mit diesem LDIF-Format zur Erweiterung des Schemas zu verwenden.

Beinhaltungsregeln

Die Objektklassen, welche die zu definierende Objektklasse enthalten können, werden im Abschnitt X-NDS_CONTAINMENT der Objektklassenbeschreibung aufgeführt. Die Objektklasse person kann in den Objektklassen organization, organizationalUnit und domain enthalten sein.

5.3.2 Neues Attribut hinzufügen

Zum Hinzufügen eines Attributs fügen Sie einfach einen Attributwert hinzu, welcher der Spezifikation für NDSAttributeTypeDescription für das Attribut „attributes“ von subschemaSubentry entspricht.

```
NDSAttributeTypeDescription = "(" whsp
  numericoid whsp  ; AttributeType identifier
  [ "NAME" qdescrs ]  ; name used in AttributeType
  [ "DESC" qdstring ]  ; description
  [ "OBSOLETE" whsp ]
  [ "SUP" woid ]  ; derived from this other AttributeType
  [ "EQUALITY" woid]  ; Matching Rule name
  [ "ORDERING" woid]  ; Matching Rule name
  [ "SUBSTR" woid ]  ; Matching Rule name
  [ "SYNTAX" whsp noidlen whsp ] ;  Syntax OID
  [ "SINGLE-VALUE" whsp ]  ; default multi-valued
  [ "COLLECTIVE" whsp ]  ; default not collective
  [ "NO-USER-MODIFICATION" whsp ] ;  default user modifiable
  [ "USAGE" whsp AttributeUsage ] ;  default userApplications
  [ "X-NDS_PUBLIC_READ" qdstrings ]
                           ; default not public read ('0')
  [ "X-NDS_SERVER_READ" qdstrings ]
                            ; default not server read ('0')
  [ "X-NDS_NEVER_SYNC" qdstrings ]
                             ; default not never sync ('0')
  [ "X-NDS_NOT_SCHED_SYNC_IMMEDIATE" qdstrings ]
                          ;  default sched sync immediate ('0')
  [ "X-NDS_SCHED_SYNC_NEVER" qdstrings ]
                                ;  default schedule sync ('0')
  [ "X-NDS_LOWER_BOUND" qdstrings ]
                            ;  default no lower bound('0')
                                  ;(upper is specified in SYNTAX)
  [ "X-NDS_NAME_VALUE_ACCESS" qdstrings ]
                       ; default not name value access ('0')
  [ "X-NDS_NAME" qdstrings ]  ; legacy NDS name
  whsp ")"
```

Die folgende LDIF-Beispieldatei fügt den Attributtyp title zum Schema hinzu:

```
1 version: 1
2 dn: cn=schema
3 changetype: add
4 attributeTypes: ( 2.5.4.12 NAME 'title' DESC 'Standa
5  rd Attribute' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{
6  64} X-NDS_NAME 'Title' X-NDS_NOT_SCHED_SYNC_IMMEDIA
7  TE '1' X-NDS_LOWER_BOUND '1')
8
```

Einwertige und mehrwertige Attribute

Attribute werden standardmäßig als mehrwertige Attribute voreingestellt, außer sie werden ausdrücklich als einwertig definiert. Im folgenden Beispiel wird in der LDIF-Datei der Titel als einwertig definiert, indem das Schlüsselwort SINGLE-VALUE nach dem Abschnitt SYNTAX hinzugefügt wird:

```
1 version: 1
2 dn: cn=schema
3 changetype: add
4 attributeTypes: ( 2.5.4.12 NAME ’title’ DESC ’Standa
5  rd Attribute’ SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{
6  64} SINGLE-VALUE X-NDS_NAME ’Title’ X-NDS_NOT_SCHED
7  _SYNC_IMMEDIATE ’1’ X-NDS_LOWER_BOUND ’1’)
8
```

Optionales Attribut zu einer vorhandenen Objektklasse hinzufügen

Das Hinzufügen neuer Schema-Elemente ist im Allgemeinen akzeptabel, aber das Ändern oder Erweitern vorhandener Schema-Elemente ist normalerweise gefährlich. Jedes Schema-Element wird eindeutig durch eine OID identifiziert. Wenn Sie deshalb ein Standardschema-Element erweitern, erstellen Sie im Prinzip eine zweite Definition für das Element, obwohl das Element weiterhin die ursprüngliche OID verwendet. Dies kann zu Inkompatibilitätsproblemen führen.

Es gibt Situationen, in denen Schema-Elemente geändert werden sollten. Beispielsweise müssen Sie neue Schema-Elemente erweitern oder ändern, wenn Sie sie während der Entwicklung verfeinern. Anstatt neue Attribute direkt zu einer Klasse hinzuzufügen, sollten Sie im Allgemeinen Zusatzklassen nur in folgenden Fällen verwenden:

- Neue Attribute zu einer vorhandenen Objektklasse hinzufügen.
- Für eine vorhandene Objektklasse eine Unterklasse erstellen.

5.3.3 Hinzufügen und Entfernen von Zusatzklassen

Die folgende LDIF-Beispieldatei erstellt zwei neue Attribute und eine Zusatzklasse mit diesen neuen Attributen. Sie fügt dann einen `inetOrgPerson`-Eintrag mit der Objektklasse `auxiliary` und mit Werten für das Zusatzklassenattribut `auxiliary` hinzu.

```
version: 1
# Add an attribute to track a bear’s hair. The attribute is
# multi-valued, uses a case ignore string syntax,
# and has public read rights
# Values may include: long hair, short, curly, straight,
# none, black, and brown
# X-NDS_PUBLIC_READ ’1’ The 1 allows public read,
# 0 denies public read
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.186.4.10 NAME
’bearHair’ SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
X-NDS_PUBLIC_READ ’1’ )

# add an attribute to store a bear’s picture
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.186.4.11 NAME
’bearPicture’ SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
SINGLE-VALUE )

# create an Auxiliary class for the bearfeatures
dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: (2.16.840.1.113719.1.186.6.101 NAME
’bearFeatures’ MAY (bearHair $ bearPicture) AUXILIARY)

# now create a user named bobby
dn: cn=bobby,o=bearcave
```

```
changetype: add
cn: bobby
sn: bear
givenName: bobby
bearHair: Short
bearHair: Brown
bearHair: Curly
bearPicture:< file:///c:/tmp/alien.jpg
objectClass: top
objectClass: person
objectClass: inetOrgPerson
objectClass: bearFeatures

# now create a person named john that will later be changed
# into a bear when bearFeatures is added to its objectClass
# list
dn: cn=john,o=bearcave
changetype: add
cn: John
sn: bear
givenName: john
objectClass: top
objectClass: person
objectClass: inetOrgPerson

# now morph john into a bear by adding bearFeatures
dn: cn=john,o=bearcave
changetype: modify
add: objectClass
objectClass: bearFeatures
-
add: bearHair
bearHair: long
bearHair: black
#bearPicture:< file:///c:/tmp/john.jpg>
-

# to morph john back to a person, simply delete the
# objectClass bearFeatures
dn: cn=john,o=bearcave
changetype: modify
delete: objectClass
objectClass: bearFeatures
```

Beim Entfernen von Zusatzklassen ist es nicht erforderlich, alle mit der Klasse `auxiliary` verknüpften Werte zu löschen, wenn Sie die Klasse `auxiliary` aus der Objektklassenliste entfernen. eDirectory führt dies automatisch aus.

Wenn die Klasse `auxiliary` über Attribute der Kategorie `MUST` verfügte, müssen diese Attribute alle im gleichen Änderungsvorgang angegeben werden, mit dem die Klasse `auxiliary` zur Objektklassenliste hinzugefügt wird. Andernfalls tritt ein Fehler bei der Änderung auf.

Bekannte Probleme bei der XML-Analyse

Die XML-Verarbeitung eines LDIF-Datensatzes (LDIF-Format oder vom LDAP-Server generierte Datensätze) kann nur erfolgreich ausgeführt werden, wenn alle einzelnen Datensätze alle in der XML-Datei angegebenen XML-Regeln erfüllen.

5.4 ldif2dib-Beschränkungen

- Abschnitt 5.4.1, „LDIF mit einfachem Passwort“, auf Seite 45
- Abschnitt 5.4.2, „Schema“, auf Seite 45

5.4.1 LDIF mit einfachem Passwort

Beim Upload von LDIF mit einfachem Passwort unter Windows tritt bei ldif2dib möglicherweise ein Fehler auf, wenn die NICI-Schlüssel in den Ordnern `system` und *`Administrator`* nicht synchronisiert sind.

Um dieses Problem zu umgehen, verwenden Sie folgende Prozedur, um auf die Schlüssel im Ordner `nici/system` zuzugreifen:

1. Öffnen Sie den Ordner `C:\Windows\system32\novell\nici\` (für die 32-Bit-Version von NICI).

   oder

   Öffnen Sie den Ordner `C:\Windows\SysWOW64\novell\nici\` (für die 64-Bit-Version von NICI).
2. Sichern Sie die Dateien im Ordner *`Administrator`*.
3. Wechseln Sie zur Registerkarte *Sicherheit* im Fenster „Eigenschaften“ des Systemordners.
4. Wählen Sie *Erweiterte Optionen* aus und wechseln Sie zur Registerkarte *Eigentümer*.
5. Wählen Sie *Administrator* aus.
6. Wechseln Sie wieder zur Registerkarte *Sicherheit* und fügen Sie „Administrator“ in der Liste hinzu.
7. Wiederholen Sie Schritt 3 bis Schritt 6, um Lesezugriff auf alle Dateien im Systemordner zu erhalten.
8. Überschreiben Sie die Dateien im Ordner *`Administrator`* mit den Dateien im Ordner `system`.
9. Nachdem der Upload abgeschlossen ist, kopieren Sie die gesicherten Dateien in den Ordner *`Administrator`*.
10. Ändern Sie den Zugriff des Administrators auf den Ordner `system` und die im Ordner enthaltenen Dateien.

5.4.2 Schema

Die LDIF-Datei sollte alle Objektklassen enthalten, zu denen ein Eintrag gehört. Darüber hinaus sollten Sie die Klassen hinzufügen, zu denen ein Eintrag aufgrund der Klassenvererbung gehört. Beispiel: Ein Eintrag vom Typ `inetOrgPerson` weist in der LDIF-Datei die folgende Syntax auf:

- `objectclass: inetorgperson`
- `objectclass: organizationalPerson`
- `objectclass: person`
- `objectclass: top`

5.4.3 ACL-Schablonen

Objekte, die bei der Verarbeitung sehr großer Datenmengen mit dem Dienstprogramm `ldif2dib` verarbeitet wurden, werden nicht mit ACLs hinzugefügt, die in den ACL-Schablonen für die Objektklasse des Objekts angegeben sind.

5.4.4 Signalbehandlungsroutine

Sie können die Bulkload-Operation zeitweise aussetzen, indem Sie die Taste s oder S drücken. Mit der Esc-Taste kann die Bulkload-Operation gestoppt werden.

6 Fehlerbehebung für SNMP

Dieser Abschnitt enthält Informationen zur Fehlerbehebung von SNMP auf beliebigen Plattformen.

6.1 Traps werden unter Umständen nicht wie erwartet generiert

Traps werden nur gesendet, wenn der Server die entsprechende Verbanforderung empfängt. In allen anderen Fällen werden keine Traps gesendet. Beispielsweise wird `ndsDeleteAttribute` nur gesendet, wenn die Anforderung `ndsRemoveEntry` (Trap Nummer 108) gesendet wird. Eine Anwendung kann jedoch immer die ACLs lesen und so prüfen, ob der Benutzer über ausreichende Rechte zum Ausführen des Löschvorgangs verfügt. In diesem Fall wird der Trap `ndsDeleteAttribute` nicht generiert. Sie können die Verbstatistiken auf einem bestimmten Server jedoch mit iMonitor anzeigen.

Um die Traps für alle Vorkommnisse abzurufen, setzen Sie das Zeitintervall auf null.

Sie können festlegen, dass Traps nur bei einer Fehlerbedingung gesendet werden. Alternativ können Sie festlegen, dass Traps unter allen Bedingungen gesendet werden.

„ndssnmpsa“ muss bei einem Neustart des Master-Agenten neu gestartet werden

Um ndssnmpsa neu zu starten, beenden Sie ndssnmpsa zunächst und führen Sie dann den Neustart durch.

Zum Beenden von ndssnmpsa geben Sie Folgendes ein:

Linux: `/etc/init.d/ndssnmpsa stop`

Zum Starten von ndssnmpsa geben Sie Folgendes ein:

Linux: `/etc/init.d/ndssnmpsa start`

6.2 SNMP-Gruppenobjekt

Wenn die Installation des SNMP-Gruppen- objekts fehlschlägt, können Sie dieses Problem beheben, indem Sie an der Server- konsole folgenden Befehl ausführen:

```
ndsconfig add -m snmp
```

6.3 SNMP-Initialisierungsfehler

eDirectory SNMP Initialization component. Error code: -255 (Fehlercode:-168)

Alternativ:

Initialization failure. Error code: -255

Eine mögliche Ursache für diesen Fehler ist die fehlende Angabe von `hostname:port` oder `IP_address:port` als Parameter im Befehl `SERVER` in der eDirectory-SNMP-Konfigurationsdatei.

Die eDirectory-SNMP-Konfigurationsdatei trägt den Namen `ndssnmp.cfg`. Sie befindet sich in folgendem Verzeichnis:

- Linux: `/etc/opt/novell/eDirectory/conf/ndssnmp/`
- Windows: *`install_directory`*`\SNMP\`

6.4 SNMP-Subagent wird nicht gestartet

Beim Starten des SNMP-Subagenten kann ein Segmentierungsfehler auftreten. Dies kann durch zusätzliche Freiräume in der Datei `ndssnmp.cfg` verursacht werden. Entfernen Sie die Freiräume und starten Sie „ndssnmpsa" neu.

6.5 LDAP-SNMP-Statistiken nicht berichtet

Wenn die anonyme Bindung deaktiviert ist, werden keine LDAP-SNMP-Statistiken berichtet.

So beheben Sie dieses Problem:

1. Erlauben Sie die anonyme Bindung.
2. Starten Sie den Subagenten.
3. Deaktivieren/verweigern Sie die anonyme Bindung.

6.6 Segmentationsfehler beim Zugriff auf den Subagenten

Wenn ein Benutzer den Subagenten (`ndssnmpsa`) startet und dabei ein falsches eDirectory-Passwort eingibt, tritt ein Segmentierungsfehler auf.

Sie vermeiden diesen Fehler, wenn Sie sicherstellen, dass Sie beim Starten des Subagenten das korrekte eDirectory-Passwort eingeben.

6.7 SNMP-Probleme

6.7.1 Probleme nach der Aufrüstung von eDirectory 8.7.3 auf eDirectory 8.8

Nach der Aufrüstung von eDirectory 8.7.3 auf eDirectory 8.8 erhalten Sie möglicherweise die folgende Fehlermeldung:

```
%%% Attempting to restart the NetIQ eDirectory SNMP subagent (ndssnmpsa)...
Starting NDS SNMP Subagent ...
Initialization failure. Error code : -255
Please Wait...
Done

%%% Unable to start ndssnmpsa... Please try starting it manually...
```

Dieser Fehler tritt auf, da eDirectory 8.8 localhost nicht überwacht. Früher war `SERVER localhost` in der Datei `ndssnmp.cfg`standardmäßig festgelegt.

Zur Behebung dieses Fehlers bearbeiten Sie die Datei `ndssnmp.cfg` manuell und fügen Sie den Hostnamen des eDirectory-Servers ein, der überwacht werden muss.

Geben Sie beispielsweise Folgendes in die Datei `ndssnmp.cfg` ein:

```
SERVER test-server
```

„test-server“ ist der Hostname, unter dem eDirectory an dem NCP-Standardport (524) ausgeführt wird. Wird eDirectory an einem anderen Port (z. B. 1524) ausgeführt, sollte der Eintrag folgendermaßen aussehen:

```
SERVER test-server:1524
```

6.7.2 Fehler beim Starten des NDS-Subagenten

Beim Starten gibt der Subagent unter Umständen folgende Fehlermeldung aus:

```
Unable to load library: libnetsnmp.so
```

Um dieses Problem zu lösen, exportieren Sie die Umgebungsvariable SNMP_MAJOR_VERSION mit der Hauptversionsnummer der net-snmp-Bibliothek (`libnetsnmp.so`). Beispiel: Führen Sie folgenden Befehl aus:

```
export SNMP_MAJOR_VERSION=10
```

6.7.3 Neustart von ndssnmpsa

Wenn der Master-Agent unter Linux neu gestartet wird, muss „ndssnmpsa“ ebenfalls neu gestartet werden.

Um ndssnmpsa neu zu starten, beenden Sie ndssnmpsa zunächst und führen Sie dann den Neustart durch.

Zum Beenden von „ndssnmpsa“ geben Sie folgenden Befehl ein:

```
/etc/init.d/ndssnmpsa stop
```

Zum Starten von ndssnmpsa geben Sie Folgendes ein:

```
/etc/init.d/ndssnmpsa start
```

6.7.4 Fehler beim Starten von ndssnmpsa

Wenn Sie „ndssnmpsa·unter Linux starten, erhalten Sie möglicherweise folgende Fehlermeldungen:

```
Error: eDirectory SNMP Initialization component. Error code: -168
```

```
Error: eDirectory SNMP Initialization component. Error code: 9
```

Um diese Fehler zu beheben, entladen und laden Sie „ndssnmp“ mit den folgenden Befehlen:

```
/opt/novell/eDirectory/bin/ndssnmp -u
```

```
/opt/novell/eDirectory/bin/ndssnmp -l
```

6.7.5 Fehler beim Stoppen von ndssnmpsa

Beim Stoppen von ndssnmpsa unter SLES 9 wird eine Fehlermeldung ähnlich der folgenden angezeigt: `"*** glibc detected *** double free or corruption (!prev): 0x0819cdd0 ***"`.

Diese Meldungen können ignoriert werden.

6.7.6 Kompilieren von edir.mib

Die MIB-Datei von eDirectory (`<`*`Stammverzeichnis_eDirectory-Installation`*`>\snmp\edir.mib)` unter Windows wird mit einigen Fehlern und Warnungen zu HP-OpenView kompiliert. Diese Fehler können Sie ignorieren.

6.7.7 SNMP-Konfigurationsdatei bearbeiten

Wenn LDAP nicht für die Ausführung im Klartextmodus konfiguriert ist, muss der Name der Datei mit dem Herkunftsverbürgungszertifikat in der SNMP-Konfigurationsdatei (z. B. SSLKEY `C:\Novell\nds\trust.der`) angegeben werden, bevor der eDirectory SNMP-Subagent gestartet wird.

`ndssnmp.cfg` finden Sie unter Windows im Verzeichnis `C:\novell\nds\snmp`.

6.7.8 Verwenden von SNMP nach der Installation eines neuen Baums

Wenn eDirectory 8.8 SP8 erstmalig installiert wird (Erstellen eines neuen Baums), kann eDirectory den SNMP-Dienst nicht herunterfahren, falls der SNMP-Dienst von Windows auf dem Server installiert ist und ein oder mehrere Dienste von dem SNMP-Dienst abhängig sind. Wenn dies passiert, ist SNMP nach der Installation von eDirectory nicht einsatzbereit.

Gehen Sie folgendermaßen vor, um den SNMP-Dienst neu zu starten:

1. Klicken Sie auf *Start* > *Einstellungen* > *Systemsteuerung* > *Verwaltung* > *Dienste*.
2. Klicken Sie in der Spalte *Name* mit der rechten Maustaste auf *SNMP-Dienst* und klicken Sie dann auf *Beenden*.
3. Klicken Sie auf *Ja, alle*.
4. Klicken Sie in der Spalte *Name* mit der rechten Maustaste auf *SNMP-Dienst* und klicken Sie dann auf *Starten*.

6.7.9 Fehler beim Erstellen von SNMP-Objekt unter Windows Server

Wenn Sie während der Installation von eDirectory auf einem Server mit unterstützter Windows-Plattform eine Fehlermeldung mit Bezug auf die Erstellung eines SNMP-Gruppenobjekts erhalten, müssen Sie das SNMP-Gruppenobjekt manuell erstellen. Informationen zu den Schritten, mit denen ein SNMP-Objekt manuell erstellt wird, finden Sie im Abschnitt „eDirectory und SNMP“ (http://www.netiq.com/documentation/edir88/edir88/data/ag7hr1h.html) im *Novell eDirectory 8.8 SP8-Administrationshandbuch)*.

6.7.10 Deinstallieren von SNMP bei der Deinstallation von eDirectory

Wenn der SNMP-Dienst von Windows auf einem Server installiert ist und der SNMP-Dienst über einen oder mehrere abhängige Dienste verfügt, werden bei der Deinstallation von eDirectory nicht alle SNMP-Dateien im Ordner `C:\novell\nds` gelöscht. Die übrigen Deinstallationsprozesse werden jedoch ordnungsgemäß abgeschlossen. Hierzu zählen unter anderem das Löschen der SNMP-Registrierungseinträge sowie der Dekonfigurationsprozess, den der NetIQ-SNMP-Agent mit DS und dem SNMP-Dienst ausführt.

So führen Sie die Deinstallation durch:

1. Klicken Sie auf *Start* > *Einstellungen* > *Systemsteuerung* > *Verwaltung* > *Dienste*.
2. Klicken Sie in der Spalte *Name* mit der rechten Maustaste auf *SNMP-Dienst* und klicken Sie dann auf *Beenden*.
3. Klicken Sie auf *Ja, alle*.
4. Klicken Sie in der Spalte *Name* mit der rechten Maustaste auf *SNMP-Dienst* und klicken Sie dann auf *Starten*.
5. Löschen Sie die verbleibenden SNMP-Dateien im Ordner `C:\novell\nds`.

7 iMonitor

7.1 Suchen nach Objekten mit Doppelbyte-Zeichen in iMonitor

Wenn Sie mithilfe von iMonitor einen eDirectory-Baum nach Objekten durchsuchen, kann es bei Objekten mit Doppelbyte-Zeichen im Namen vorkommen, dass die Hyperlink-Verknüpfung zu den Objekteigenschaften nicht richtig funktioniert.

7.2 Agentenstatusprüfung für einen Baum mit nur einem Server

Bei Ausführung der Funktion zur Agentenstatusprüfung von iMonitor auf einem Baum mit nur einem Server kommt es aufgrund des Status "Befristete Daten" zur Anzeige eines Warnsymbols in der Ergebnisspalte. Das bedeutet jedoch nicht, dass der Zustand des Baums gefährdet ist oder dass die Agentenstatusprüfung nicht wie vorgesehen funktioniert. Der Status "Befristete Daten" gibt die Datenmenge an, die noch nicht mit mindestens einer Reproduktion synchronisiert wurde. Ein Baum mit nur einem Server bedeutet von Natur aus, dass die Daten bei schweren Fehlern immer gefährdet sind, weil sie an keine andere Stelle reproduziert worden sind. Wenn die Festplatte beschädigt wird, sind die Daten verloren.

Wenn Sie keine Statusprüfungswarnungen über gefährdete Daten oder die Anzahl lesbarer Reproduktionen auf Ihrem Einzelserver-Baum anzeigen möchten, können Sie diese Statusprüfungen deaktivieren, indem Sie in der Datei `ndsimonhealth.ini` die folgenden Einträge wie dargestellt ändern:

```
perishable_data-active: OFF
```

und

`ring_readable-Min_Marginal: 1` oder `ring_readable-active: OFF`

Damit werden die Warnungen für die Anzahl lesbarer Reproduktionen und befristete Daten deaktiviert.

7.3 Der iMonitor-Bericht speichert nicht die Datensätze für jede Stunde

Die iMonitor-Funktion zur benutzerdefinierten Berichterstellung ist so ausgelegt, dass die vom Benutzer angegebene URL beim Erstellen des Berichts in den gespeicherten Bericht (die gespeicherte HTML-Datei) platziert wird. Das bedeutet, dass Sie beim Öffnen eines gespeicherten benutzerdefinierten Berichts anstelle der von der URL zum Zeitpunkt der Berichterstellung erfassten Daten die Live-Daten (d. h. die aktuellen Daten) sehen. Dieses Problem wird mit einer künftigen Version von iMonitor gelöst.

7.4 Erstellungs- und Änderungszeitstempel

Da auf Linux-Plattformen das Erstellungsdatum einer Datei nicht angegeben wird, zeigt iMonitor das Erstellungs- und das Änderungsdatum als das gleiche Datum an.

7.5 Probleme mit iMonitor bei älteren Versionen von Mozilla

Wenn Sie mit einer älteren Mozilla-Version als Version 1.5 auf iMonitor zugreifen, treten in iMonitor bei der DSTrace-Flaggenauswahl möglicherweise Probleme auf. Mozilla unterstützt möglicherweise nicht alle Vorgänge.

7.6 Ausführen des Berichtbildschirmlayouts nicht auf iMonitor ausgerichtet

Die Navigations- und Assistentenrahmen erscheinen unter Linux zweimal.

Diese Problem lässt sich durch Aktualisieren der Seite umgehen.

7.7 iMonitor zeigt Fehler -672 an

Bei einigen Operationen tritt ein Fehler auf und es wird der Fehler -672 angezeigt, wenn parallel zu iMonitor ein Werkzeug zur Fehlersuche ausgeführt wird.

Unter Linux

iMonitor zeigt den Fehler -672 an, wenn das dsdump-Werkzeug parallel zu iMonitor ausgeführt wird.

Um das Problem zu beheben, beenden Sie das dsdump-Werkzeug, bevor Sie iMonitor starten.

Unter Windows

iMonitor zeigt den Fehler -672 an, wenn das dsbrowse- oder dsedit-Werkzeug parallel zu iMonitor ausgeführt wird.

Um das Problem zu beheben, beenden Sie das dsbrowse- bzw. dsedit-Werkzeug, bevor Sie iMonitor starten.

7.8 Zeitstempel werden im Hexadezimalformat angezeigt

Wenn Sie ein Zeitsyntaxattribut mit einem Wert vor dem 1. Januar 1970 festlegen, zeigt iMonitor den Zeitstempel des Attributs im Hexadezimalformat und nicht im Datums-/Uhrzeitstandardformat an. iMonitor zeigt alle Attribute mit Werten nach dem 1. Januar 1970 im Datums-/Uhrzeitformat an.

7.9 Problem mit iMonitor-Trace-Konfiguration in Internet Explorer 10

Die Trace-Konfiguration in iMonitor funktioniert in Internet Explorer 10 nicht.

Um das Problem zu umgehen, starten Sie Internet Explorer 10 im Kompatibilitätsmodus und fügen Sie die iMonitor-Adresse zur Liste der vertrauenswürdigen Sites hinzu. Starten Sie den Browser anschließend neu.

8 iManager

8.1 LDAP-Operationen schlagen fehl, nachdem ein neues LDAP-Gruppenobjekt mit Quick Create erstellt wurde

Quick Create erstellt nur ein LDAP-Gruppenobjekt mit Pseudoattributen, die Sie später ändern können. Das LDAP-Gruppenobjekt wird dabei mit Version elf anstelle von Version zwölf erstellt. Daher schlagen alle LDAP-Operationen fehl, da die Zuordnung eines LDAP-Servers aufgrund der Versionsinkompatibilität nicht möglich ist.

Dieses Problem lässt sich umgehen, indem Sie nach dem Erstellen des LDAP-Gruppenobjekts mit Quick Create die Versionsnummer des LDAP-Gruppenobjekts in zwölf ändern.

9 Nachrufe

Nachrufe werden als operationale Attribute eingesetzt, die eDirectory Objekten zuweist, um die referenzielle Integrität bei Vorgängen wie dem Löschen, Verschieben, Umbenennen oder Wiederherstellen zu gewährleisten. Wenn zum Beispiel eine Gruppe A über das Mitglied „Benutzer B“ verfügt und Benutzer B gelöscht wird, entfernt das Verzeichnis automatisch den Bezug zu Benutzer B von Gruppe A. In eDirectory 8.8 SP8 werden die Nachrufe, die von den Lösch-, Verschiebungs- und Umbenennungsvorgängen generiert werden, standardmäßig optimiert.

HINWEIS: Objekte mit Nachrufen werden immer dann in Betracht gezogen, wenn ein Agent ausgehend synchronisiert. Sie werden auch vom Nachrufvorgang in Betracht gezogen, der planmäßig am Ende eines Eingangssynchronisierungszyklus ausgeführt wird.

Es gibt drei allgemeine Klassifizierungen für Nachrufe:

- Primäre Nachrufe umfassen die Typen „Inaktiv“ (0001), „Wiederhergestellt" (0000), „Verschoben“ (0002), „Neue RDN“ (0005) und „Baum neue RDN“ (0008).
- Sekundäre Nachrufe sind in der Regel mit einem primären Nachruf verknüpft und stellen die Agenten und Partitionen dar, die über den im primären Nachruf angegebenen Vorgang benachrichtigt werden müssen. Sekundäre Nachrufe umfassen die Typen „Backlink“ (0006), „Genutzt durch“ (000C) und „Baum verschieben“ (000a).
- Verfolgungsnachrufe umfassen die Typen „Verschieben sperren“ (0003), „Alte RDN“ (0004) und „Baum alte RDN“ (0007).

Abgesehen von den Verfolgungsnachrufen müssen Nachrufe eine Reihe von Synchronisierungszuständen durchlaufen.

- "Ausgangszustand" oder "Ausgestellt" (0)
- "Benachrichtigt" (1)
- „Tilgen bestätigt“ (2)
- "Entfernbar" (4)

Die Zustände werden im Flaggenfeld im Nachrufattribut protokolliert. Bevor ein Nachruf in den nächsten Zustand übergehen kann, muss der aktuelle Zustand mit allen Reproduktionen des echten Objekts synchronisiert sein. Um festzustellen, ob alle Reproduktionen im Ring einen gegebenen Nachrufzustand erkannt haben, wird anhand des transitiven Vektors ein Vektor berechnet. In eDirectory 8.6 wird ein nicht gespeicherter Nachrufvektor verwendet. In früheren Versionen von eDirectory wird der Entfernvektor verwendet. Wenn der Änderungszeitstempel (MTS) auf dem Nachruf älter als der berechnete Vektor ist, so kann der Server, der für diesen Nachruf zuständig ist, diesen in den nächsten Zustand überführen.

Für einen sekundären Nachruf vom Typ "Backlink" ist der Agent, der die Masterreproduktion des Objekts mit dem Nachruf enthält, dafür zuständig, den Nachruf in die nächsten Zustände zu versetzen. Für einen sekundären Nachruf vom Typ "Genutzt durch" ist der Reproduktionsagent, der ihn erstellt hat, dafür zuständig, den Nachruf in die nächsten Zustände zu befördern, und zwar so lange wie die Reproduktion besteht. Wenn die Reproduktion nicht mehr vorhanden ist, so übernimmt es der Agent mit der Masterreproduktion dieser Partition, den Nachruf vom Typ

"Genutzt durch" in die nächsten Zustände zu versetzen. Bei einem Nachruf vom Typ "Baum verschieben" ist die Masterreproduktion der Stammpartition dafür zuständig, den Nachruf in die nächsten Zustände zu versetzen.

Primäre Nachrufe können nur dann in die nächsten Zustände versetzt werden, wenn alle sekundären Nachrufe alle Zustände durchlaufen haben. Wenn ein primärer Nachruf seinen letzten Zustand erreicht hat und dieser Zustand mit allen Servern im Ring synchronisiert ist, so bleibt nur die Objekthülle übrig, also ein Objekt ohne Attribute, das anschließend durch den Tilgungsvorgang aus dem System entfernt werden kann. Verfolgungsnachrufe werden entfernt, sobald der primäre Nachruf entfernt werden kann. Bei `Inhibit_move` (Verschieben unterbinden) wird der Verfolgungsnachruf entfernt, sobald der primäre Nachruf in den Zustand `OBF_NOTIFIED` auf der Masterreproduktion übergegangen ist.

Die für die Verarbeitung der Nachrufe zuständige Reproduktion erledigt dies im Hintergrund (im Nachrufvorgang), der auf pro-Partition-Basis geplant ist und ausgeführt wird, wenn eine gegebene Partition einen Eingangssynchronisierungszyklus abgeschlossen hat. Sind keine anderen Reproduktionen der Partition vorhanden, so wird der ausgehende Reproduktionsvorgang weiterhin im Heartbeat-Intervall geplant. Der ausgehende Reproduktionsvorgang startet dann den Nachrufvorgang. Der Nachrufvorgang kann nicht manuell geplant werden, was jedoch auch nicht erforderlich ist. Bei der Synchronisierung werden die transitiven Vektoren aktualisiert und geben den Entfernvektor und den Nachrufvektor weiter. Wenn diese Vektoren in den nächsten Zustand versetzt werden, können die Nachrufe ebenfalls in die nächsten Zustände übergehen. Zusammen mit der automatischen Planung durch die Eingangssynchronisierung schließt dies den Nachrufvorgangszyklus ab. Somit stellt die Objektsynchronisierung den Lebensnerv der Nachrufverarbeitung dar.

Nachdem alle Nachrufe, deren verknüpfte primäre Nachrufe vom Typ „Inaktiv“ sind, in den letzten Zustand (Entfernbar) versetzt wurden und dieser Zustand mit allen Reproduktionen synchronisiert wurde, ist nun für ein Objekt, das entfernt wird, ein neuer Vorgang zur Entfernung der verbleibenden Eintragshülle aus der Datenbank zuständig. Der Entfernvorgang wird automatisch ausgeführt, um diese Hüllen zu entfernen. Auf der Seite Agentenkonfiguration in iMonitor kann der Entfernvorgang manuell geplant und sein automatisches Planintervall geändert werden.

9.1 Beispiele

Dieser Abschnitt enthält die folgenden Beispiele:

- „Objekt löschen“, auf Seite 60
- „Objekt verschieben“, auf Seite 61

9.1.1 Objekt löschen

1 Primären Nachruf OBT_DEAD hinzufügen.

   Das Backlink-Attribut enthält eine Liste der Server, die ein Interesse an diesem Objekt haben und über Änderungen dieses Eintrags benachrichtigt werden müssen. Für jeden DN, der im Backlink-Attribut aufgeführt ist, und für alle Server, die im Partitionsreproduktionsattribut des Eintrags aufgeführt sind, fügt eDirectory einen Backlink-Nachruf hinzu. Der Zeitpunkt der Erstellung des primären Nachrufs, nämlich OBT_DEAD, wird im sekundären Nachruf gespeichert.

Das Attribut "Genutzt durch" enthält eine Liste der Server, die ein Interesse an diesem Objekt haben und über Änderungen dieses Eintrags benachrichtigt werden müssen. Für jeden DN, der im Attribut "Genutzt durch" aufgeführt ist, fügt eDirectory einen Nachruf "Genutzt durch" hinzu. Der Zeitpunkt der Erstellung des primären Nachrufs, nämlich OBT_DEAD, wird im sekundären Nachruf gespeichert.

2 Entfernen aller Attribute außer der Nachrufe.

   Der ausgehende Reproduktionsvorgang synchronisiert dann diese Änderung mit allen anderen Servern im Reproduktionsring.

   Bei der nächsten Eingangssynchronisierung dieser Partition wird der Nachrufvorgang gestartet, der Folgendes ausführt:

   - Er berechnet einen Zeitvektor, der ein minimaler transitiver Vektor ist und als Entfernvektor bezeichnet wird. Spätere Versionen von eDirectory berechnen einen zweiten minimalen Vektor, der als Nachrufvektor bezeichnet wird und keine Reproduktionen berücksichtigt, die untergeordnete Referenzen sind.
   - Jeder Nachruf in dieser Partition wird nun untersucht.

     Wenn der Nachruf ein primärer Nachruf ist, es keine sekundären Nachrufe gibt und die Änderungszeit (MTS) des Attributs im Nachruf älter als der Entfernvektor ist, so haben alle Server diese Änderung erfasst und dieser Nachruf wird entfernt.

     Wenn es sich bei dem Nachruf um einen Backlink-Nachruf handelt und dieser Server der Master ist, so ist dieser Server für die Verarbeitung dieses Nachrufs zuständig.

     WICHTIG: Durchführung des für diesen Zustand erforderlichen Vorgangs, falls noch nicht erfolgt. In den meisten Fällen erfolgt dies durch Benachrichtigung eines externen Verweises.

     Wenn der Nachruf ein Nachruf vom Typ „Genutzt durch“ ist und dieser Server der Server ist, auf dem der Löschvorgang ausgeführt wurde (was durch Vergleichen der Reproduktionsnummer in der Änderungszeit (MTS) im Nachruf mit unserer Reproduktionsnummer festgestellt wird), so ist dieser Server für die Verarbeitung dieses Nachrufs zuständig.
   - Wenn dieser Server für die Verarbeitung eines bestimmten sekundären Nachruftyps („Backlink“ oder „Genutzt durch“) zuständig ist, sich alle sekundären Nachrufe dieses Typs in einem Eintrag im selben Zustand befinden, der für diesen Zustand erforderliche Vorgang bei allen Nachrufen durchgeführt wurde (zum Beispiel die Benachrichtigung der Server) und die Änderungszeiten des Nachrufs für diesen Nachruftyp älter als der Nachrufvektor sind, so können alle sekundären Nachrufe dieses Typs in den nächsten Zustand überführt werden.

9.1.2 Objekt verschieben

Der Vorgang „Verschieben“ ist dem Vorgang Löschen sehr ähnlich, unterscheidet sich jedoch in den folgenden Punkten davon:

- Vor Platzierung des primären Nachrufs im Ursprungseintrag für den Verschiebevorgang wird ein Teileintrag im Zielcontainer erstellt und ein Verfolgungsnachruf (OBT_INHIBIT_MOVE) in diesem Teileintrag platziert. Dieser Verfolgungsnachruf wird platziert, um zu verhindern, dass der Eintrag verschoben wird oder an einem Partitionsvorgang beteiligt ist, bevor der gesamte Eintrag aus dem Ursprung übertragen wurde.

- Der primäre Nachruf im Ursprungseintrag ist vom Typ OBT_MOVED.
- Nachdem der primäre Nachruf (OBT_MOVED) in den Zustand „Benachrichtigt“ versetzt wurde (was bedeutet, dass alle Reproduktionen des Ursprungs nun darüber informiert sind, dass der Eintrag verschoben wird) und alle externen Verweise benachrichtigt wurden, wird der Verfolgungsnachruf (OBT_INHIBIT_MOVE) aus dem Zieleintrag entfernt.

9.2 Vorbeugende Maßnahme

Erstellen Sie in regelmäßigen Abständen den Bericht "Serverinformationen in iMonitor". Dieser Bericht führt durch den gesamten Baum, kommuniziert mit jedem vorgefundenen NCP-Server und meldet alle gefundenen Fehler. Mit Hilfe dieses Berichts können Zeitsynchronisierungs- und Limberprobleme diagnostiziert werden oder es kann herausgefunden werden, ob der aktuelle Server mit allen anderen Servern aus der Sicht dieses Servers kommunizieren kann. Nach der entsprechenden Auswahl auf der Konfigurationsseite kann der Server auch für jeden Server im Baum Informationen zum NDS-Agentenzustand generieren. Weitere Informationen über das Ausführen des Serverinformationsberichts finden Sie unter „Konfigurieren und Anzeigen von Berichten“ im *NetIQ eDirectory 8.8 SP8-Administrationshandbuch*.

Wenn Sie iMonitor 2.0 oder höher verwenden, stellen Sie sicher, dass die Optionen für Fehler- und Zustands-Teilberichte aktiviert sind. Die folgenden Punkte werden überprüft. Sie sollten den Bericht durchsuchen und sicherstellen, dass keine Fehler aufgetreten sind.

- Der Bericht überprüft die eDirectory-Agentenversion auf Grundlage der Informationen, die in der `ndsimonhealth`-Konfigurationsdatei mit iMonitor (siehe „Konfigurationsdateien“ im *NetIQ eDirectory 8.8 SP8-Administrationshandbuch*) gespeichert sind, um sicherzustellen, dass im gesamten Baum die richtigen Verzeichnis-Patches ausgeführt werden.
- Alle Server liegen innerhalb der Zeitsynchronisierungs-Toleranzen.
- Dieser Server kann mit allen anderen Servern kommunizieren.
- Es wurden keine Server falsch oder unvollständig aus dem Baum entfernt.
- Im Zustands-Teilbericht wird angegeben, wenn Partitionen außerhalb der Toleranz für die Reproduktionssynchronisierungszeiten liegen.

Wenn Sie iMonitor 1.5 verwenden, wählen Sie die Berichtart "Fehler" aus. Die folgenden Punkte werden überprüft. Sie sollten den Bericht durchsuchen und sicherstellen, dass keine Fehler aufgetreten sind.

- Die Agentenversion wird angezeigt. Stellen Sie sicher, dass alle Server im gesamten Baum den aktuellsten eDirectory Support Pack ausführen, der auf der NetIQ Support-Website (http://support.novell.com) zur Verfügung steht.
- Alle Server liegen innerhalb der Zeitsynchronisierungs-Toleranzen.
- Dieser Server kann mit allen anderen Servern kommunizieren.
- Es wurden keine Server falsch oder unvollständig aus dem Baum entfernt.

Mit Hilfe der iMonitor-Berichte "Nachrufliste" oder "Objektstatistik" finden Sie alle Nachrufe, die sich auf Ihrem System befinden. Sollten Sie Nachrufe finden, die Ihrer Meinung nach nicht verarbeitet werden, beachten Sie die Abschnitt 9.3, „Tipps zur Fehlersuche“, auf Seite 63.

9.3 Tipps zur Fehlersuche

Es gibt im Allgemeinen zwei Ursachen für nicht verarbeitete Nachrufe: Der Nachruf ist entweder bezugslos (das heißt, er ist auf einigen Servern vorhanden, jedoch nicht auf allen) oder der Nachruf wurde blockiert (was bedeutet, dass er auf allen Servern vorhanden ist, aus irgendeinem Grund aber nicht in die nächsten Zustände überführt wird).

Gehen Sie bei bezugslosen oder blockierten Nachrufen zur Fehlersuche wie folgt vor:

- ❒ Keine Panik!
- ❒ Bei einem Nachruf für ein Objekt, das nicht auf diesem Server gespeichert ist (d. h. das Objekt ist ein externer Verweis):
  - Überprüfen Sie, ob das echte Objekt einen entsprechenden Nachruf besitzt. Wenn dies nicht der Fall ist, dann handelt es sich um einen bezugslosen Nachruf. Weitere Informationen finden Sie in „Bezugslose Nachrufe auf externen Verweisen auflösen“, auf Seite 64.
  - Wenn das echte Objekt einen entsprechenden Nachruf besitzt, lösen Sie Nachrufprobleme auf dem echten Objekt auf, bevor Sie versuchen, Probleme mit dem Nachruf auf der Partition des externen Verweises (`ExtRef`) zu beheben.
- ❒ Stellen Sie sicher, dass die Nachrufe korrekt synchronisiert sind.
  - Weitere Informationen zur Überprüfung und Auflösung von Synchronisierungsfehlern finden Sie auf der Seite Agentensynchronisierung von iMonitor.
  - Nachrufe können erst in andere Zustände wechseln, wenn alle Agenten mit einer Kopie des Reproduktionsrings den Zustandswechsel erfasst haben. Es gibt mehrere Möglichkeiten, um sicherzustellen, dass jede Reproduktion die Daten zur Kenntnis genommen hat:

    Beim Durchsuchen des Eintrags, in dem sich Nachrufe befinden, klicken Sie auf den Link "Eintragssynchronisierung". Die angezeigte Seite führt alle Attribute auf, die nicht mit allen Reproduktionen synchronisiert wurden.

    Suchen Sie den ältesten Zeitstempel auf einem Nachrufattributswert. Der Unterschied zwischen dieser Zeit und der aktuellen Zeit sollte größer sein als das Intervall, das im Feld "Maximaler Ringabstand" auf der Seite "Partitionssynchronisierung" angezeigt wird.

    Analysieren Sie den transitiven Vektor.
- ❒ Erstellen Sie den iMonitor-Serverinformationsbericht, um sicherzustellen, dass alle Server miteinander kommunizieren.
- ❒ Untersuchen Sie den Agentenprozessstatus: Nachrufe auf Fehler.
  - Übliche Probleme im „Agentenprozessstatus: Nachrufe“ sind

    die Kommunikationsprobleme -625, -622, -634 und -635. Weitere Informationen finden Sie unter Bericht der Serverinformationen.

    -601 und -603 geben an, dass einige Server nicht richtig entfernt wurden oder dass das Serverobjekt möglicherweise eine Basisklasse von „Unbekannt“ enthält.
  - Die auf dieser Seite angezeigten Fehler sind nicht schwerwiegend. Bei der nächsten Ausführung des Nachrufvorgangs für diese Partition wird dieser Vorgang erneut versucht. Lösen Sie alle auf dieser Seite angezeigten Probleme auf und warten Sie auf den erneuten Versuch.

- ❒ Wenn Sie sich die Nachrufobjekte ansehen, vergleichen Sie den jeweiligen Nachruf mit anderen Objekten im gesamten Ring.
    - Wenn nicht alle Reproduktionen eine Kopie des Nachrufs besitzen und nicht alle Attributwerte entfernbar sind, so ist dieses Objekt im Reproduktionsring inkonsistent, es handelt sich also um einen bezugslosen Nachruf. Weitere Informationen finden Sie in „Bezugslose Nachrufe auflösen“, auf Seite 64.
    - Wenn das Objekt in allen Reproduktionen vorhanden und konsistent ist, wird es möglicherweise aufgrund von Synchronisierungsfehlern nicht in die nächsten Zustände versetzt oder der Nachrufvorgang ist fehlerhaft.
- ❒ Verwenden Sie Trace mit der aktivierten Nachrufoption, um den Nachrufvorgang im Detail zu untersuchen.
- ❒ Um zukünftige Nachrufprobleme zu vermeiden, rüsten Sie auf das neueste Support Pack auf (für eDirectory 8.6-Server). Für alle bekannten Nachrufprobleme sind Reparaturoptionen vorhanden.

9.3.1 Lösungen

Verwenden Sie die entsprechende unter Abschnitt 9.3, „Tipps zur Fehlersuche“, auf Seite 63 angegebene Lösung.

Vor der Anwendung dieser Lösungen müssen Sie sicherstellen, dass Ihre Daten gesichert sind. Sie müssen eventuell die Verzeichnisdatenbankdateien, die Serverkonfiguration und die Trustees sichern. Um die Wahrscheinlichkeit zu erhöhen, dass die Aktion erfolgreich ist, und um zukünftige Probleme zu minimieren, rüsten Sie auf die neuesten eDirectory-Support Packs auf.

Bezugslose Nachrufe auflösen

- **Bevorzugte Methode:** Wenn eDirectory 8.6. oder höher auf einem der Server im Reproduktionsring installiert ist, wechseln Sie zu dem Objekt in iMonitor und wählen Sie die Option zum Senden eines Einzeleintrags. Dadurch wird ein nicht autorisierter Sendevorgang an alle anderen Reproduktionen ausgeführt.
- **Weit weniger wünschenswerte Methode:** Wenn alle Server im Reproduktionsring mit einer Kopie des bezugslosen Nachrufs älter sind als eDirectory 8.6, laden Sie DSBrowse mit der Option -a, wechseln Sie zum Objekt und versehen Sie den Eintrag mit einem Zeitstempel. Dadurch wird das Objekt, das sich so auf diesem Server befindet, zu einer autorisierten Kopie. Wir raten aus praktischen Gründen davon ab, Objekte zu autorisieren.

Bezugslose Nachrufe auf externen Verweisen auflösen

- **Weniger wünschenswerte Methode:** DSRepair mit aktivierter Zeitstempeloption ausführen.
- **Weniger wünschenswerte Methode:** Verschieben Sie eine echte Reproduktion auf den Server. Warten Sie auf ihren Start und die Verarbeitung des Nachrufs. Wenn der Nachruf nicht verarbeitet wird, gehen Sie entsprechend der Informationen unter Abschnitt 9.3, „Tipps zur Fehlersuche“, auf Seite 63 vor, um das Problem aufzulösen, nachdem es sich jetzt in einer echten Reproduktion befindet. Nach Verarbeitung des Nachrufs kann die Reproduktion, falls gewünscht, entfernt werden.

9.3.2 Frühere Vorgehensweisen

In der Vergangenheit wurden einige verschiedene Strategien angewandt, um blockierte Nachrufe zu lösen. Einige dieser Strategien basieren auf teuren Partitionierungsvorgängen oder verwenden nicht dokumentierte Eigenschaften, die in der Zukunft möglicherweise Probleme verursachen.

Die erste Strategie bestand darin, die Reproduktion umzustellen, auf der sich der Master befand. Dies funktioniert in einigen Fällen, da der Master der Agent ist, der dafür zuständig ist, die Backlink-Nachrufe in ihre nächsten Zustände zu versetzen. Wenn die Reproduktion inkonsistent war und der Master das gelöschte Objekt nicht enthielt, gab die Umstellung der Master auf einen Agenten, der den gelöschten Eingang mit den Nachrufen enthielt, dem neuen Agenten die Genehmigung, die Nachrufe in ihre nächsten Zustände zu versetzen und sie schließlich zu entfernen. Die Option "Einzeleintrag senden" ist eine viel sauberere und weniger gefährliche Methode zur Auflösung von Nachrufen, die aufgrund der inkonsistenten Reproduktion blockiert wurden.

Die zweite Strategie bestand darin, DSRepair mit bestimmten Parametern auszuführen, um alle Nachrufe zu löschen. (Es gibt eine Drittanbieter-Anwendung, die blockierte Nachrufe durch Starten von DSRepair löst.) Wir raten von dieser Strategie ab. Durch diese Parameter werden alle Nachrufe auf diesem Agenten gelöscht, was bedeutet, dass möglicherweise auch nicht blockierte Nachrufe entfernt und so neue inkonsistente Reproduktionen und weitere blockierte Nachrufe erzeugt werden. Da es sich hierbei nicht um eine dezentrale Operation handelt, müssen Sie DSRepair auf allen Servern mit blockierten Nachrufen ausführen, wodurch die Wahrscheinlichkeit erhöht wird, dass einer dieser Server Nachrufe für eine andere Partition enthält, die dadurch vorzeitig gelöscht werden. Wenn Nachrufe vorzeitig gelöscht werden, kann dies zusätzliche bezugslose Nachrufe erzeugen und wiederum Probleme schaffen, die erst Jahre später erkannt werden, wenn Sie Reproduktionstypen ändern, neue Reproduktionen hinzufügen oder andere Partitionsvorgänge durchführen.

Bei der dritten Strategie wurden Objekte autorisiert, indem entweder DSBrowse im erweiterten Modus ausgeführt und der Eintrag mit einem Zeitstempel versehen oder DSRepair mit dem Parameter -0T ausgeführt wurde. Dadurch wird der Eintrag gezwungenermaßen autorisiert und mit allen anderen Reproduktionen synchronisiert. Dies sollte mit äußerster Vorsicht ausgeführt werden, da Daten, die auf anderen Servern geändert wurden, verloren gehen können. Wir empfehlen, diese Methode nur im Ausnahmefall zur Bereinigung von Nachrufen zu verwenden.

10 Migration zu NetIQ eDirectory

Dieses Kapitel enthält Erläuterungen zur Migration von folgenden Systemen zu NetIQ eDirectory:

10.1 Migration vom Sun ONE-Schema zu NetIQ eDirectory

Führen Sie folgende Schritte aus, um das Sun ONE-Schema zu NetIQ eDirectory zu migrieren:

10.1.1 Schritt 1: Aktualisierungsvorgang für Schema-Cache ausführen

Mit folgendem Befehl können Sie die Fehler, die beim Vergleich des Schemas auftreten, in eine Fehlerdatei schreiben:

```
ice -e LDIF error file name -C -a -SLDAP -s Sun ONE server -p Sun ONE port -DLDAP -
s eDirectory server -p eDirectory port
```

Beispiel:

```
ice -e err.ldf -C -a -SLDAP -s sun_srv1 -p sun_port1 -DLDAP -s edir_srv2 -p
edir_port2
```

Alle beim Vergleichen des Schemas aufgetretenen Fehler werden in die Fehlerdatei (in diesem Beispiel `err.ldf`) geschrieben. Zum Ausführen dieses Vorgangs ist keine Anmeldung erforderlich, es sei denn, einer der Server benötigt zum Lesen des Root-DSE eine Authentifizierung. Microsoft Active Directory erfordert eine Authentifizierung zum Lesen des Root-DSE.

10.1.2 Schritt 2: Fehlerhafte LDIF-Datei korrigieren, um die Fehler zu beseitigen

- Sun ONE definiert bestimmte Schemadefinitionen öffentlich, die eDirectory nicht öffentlich definiert. Dies betrifft Attribute wie `objectClasses`, `attributeTypes`, `ldapSyntaxes` und `subschemSubentry`. Diese Definitionen existieren intern sind für das Schema von wesentlicher Bedeutung. Sie können daher nicht geändert werden. Vorgänge, die versuchen, diese Definitionen zu ändern, verursachen folgenden Fehler:

  ```
  LDAP-Fehler: 53 (DSA will nicht aktiv werden)
  ```

  Datensätze, die Bezüge zu diesen Definitionen enthalten, verursachen folgenden Fehler:

```
LDAP-Fehler: 16: (kein solches Attribut)
```

Datensätze, die einen Bezug zu diesen Objekten enthalten oder versuchen, diese Definitionen zu ändern, müssen in der LDIF-Fehlerdatei (in diesem Beispiel `err.ldf`) kommentiert werden.

- Einige Objektklassendefinitionen in Sun ONE verfügen über keine Benennungsattribute. Beim Hinzufügen solcher Objektklassen würde in eDirectory folgender Fehler auftreten:

  ```
  LDAP-Fehler: 80 (NDS-Fehler: keine eindeutige Benennung (-651)
  ```

  Dieser Fehler tritt auf, weil Sun ONE nicht die gleiche Methode zur Bestimmung von Benennungsregeln verwendet wie eDirectory.

  Setzen Sie *eine* beliebige der drei folgenden Optionen ein, um das Problem zu lösen:

  Option 1:

  Fügen Sie zu jeder der betreffenden Objektklassen ein gültiges Benennungsattribut hinzu.

  Beispiel:

  Um das Benennungsattribut `[ cn ]` zur Objektklasse `netscapeMachineData` hinzuzufügen, bearbeiten Sie den Eintrag (im Beispiel unten *hervorgehoben*) in der Datei `err.ldf` unter Verwendung der Flagge `X-NDS_NAMING`:

  ```
  dn: cn=schemachangetype: modifyadd: objectClassesobjectClasses: (
  2.16.840.1.113730.3.2.32 NAME 'netscapeMachineData'
      DESC 'iPlanet defined objectclass' SUP top STRUCTURAL MAY 'cn'     X-
  NDS_NAMING 'cn' )-
  ```

  Option 2:

  Definieren Sie jede betreffende Objektklasse als AUXILIARY oder ABSTRACT.

  Beispiel:

  Um die Definition der Objektklasse `netscapeMachineData` von STRUCTURAL in AUXILIARY zu ändern, bearbeiten Sie den Eintrag in der Datei `err.ldf` (im Beispiel unten *hervorgehoben*) wie folgt:

  ```
  dn: cn=schemachangetype: modifyadd: objectClassesobjectClasses: (
  2.16.840.1.113730.3.2.32 NAME 'netscapeMachineData'
     DESC 'iPlanet defined objectclass' SUP top AUXILIARY )-
  ```

  Um die Definition der Objektklasse `netscapeMachineData` von STRUCTURAL in ABSTRACT zu ändern, bearbeiten Sie den Eintrag in der Datei `err.ldf` (im Beispiel unten *hervorgehoben*) wie folgt:

  ```
  dn: cn=schemachangetype: modifyadd: objectClassesobjectClasses: (
  2.16.840.1.113730.3.2.32 NAME 'netscapeMachineData'
     DESC 'iPlanet defined objectclass' SUP top ABSTRACT )-
  ```

  Option 3:

  Fügen Sie `cn` zur Definition von `Top` in eDirectory hinzu, um ein potenzielles Benennungsattribut für alle Objektklassen zu verursachen.

  Zum Hinzufügen von `cn` zu `Top` stehen zwei Methoden zur Verfügung:

  - **Methode 1:**

    Erstellen Sie wie nachfolgend dargestellt eine Datei und benennen Sie die Datei `topsch.ldf`.

    ```
    version : 1

    dn:cn=schema

    changetype :modify
    ```

```
delete : objectclasses

objectclasses : ( 2.5.6.0 NAME 'top' STRUCTURAL )

-

add:objectclasses

objectclasses : (2.5.6.0 NAME 'top' STRUCTURAL MAY cn)
```

Führen Sie folgende NetIQ Import Conversion Export (ICE)-Befehlszeile aus:

```
ice -SLDIF -f LDIF_file_name -DLDAP -s eDirectory_server -p eDirectory_port
-d eDirectory_Admin_DN -w eDirectory_password
```

Beispiel:

```
ice -SLDIF -f topsch.ldf -DLDAP -s edir_srv2 -p edir_port2 -d
cn=admin,o=org -w pwd1
```

- **Methode 2:**

  1. Klicken Sie in NetIQ iManager auf die Schaltfläche *Rollen und Aufgaben* .
  2. Klicken Sie auf *Schema* > *Attribut hinzufügen*.
  3. Wählen Sie in der Liste *Verfügbare Klassen* den Eintrag *Anfang* und klicken Sie auf *OK*.
  4. Doppelklicken Sie in der Liste *Verfügbare optionale Attribute* auf *CN*.
  5. Klicken Sie auf *OK*.

- Einige Objektklassendefinitionen enthalten `userPassword` als Bestandteil der Liste obligatorischer Attribute. Beim Hinzufügen solcher Objektklassen zu eDirectory tritt folgender Fehler auf:

  ```
  LDAP-Fehler: 16 (kein solches Attribut)
  ```

  Um das Problem zu lösen, ändern Sie die Objektklassendefinition so, dass sie die neue Objektklasse von `ndsLoginProperties` erbt, und entfernen Sie das Attribut `userPassword` aus der Liste der obligatorischen Attribute.

  Beispiel:

  Eine Objektklasse, die `userPassword` in der Liste obligatorischer Attribute enthält:

  ```
  version : 1
  dn: cn=schemaz
  changetype: modify
  add: objectClasses
  objectClasses: ( 0.9.2342.19200300.100.4.19 NAME 'simpleSecurityObject' DESC '
   Standard LDAP objectClass' SUP top STRUCTURAL MUST userPassword )
  ```

  Dies muss folgendermaßen geändert werden (beachten Sie die Änderung in der letzten Zeile):

  ```
  version : 1
  dn: cn=schema
  changetype: modify
  add: objectClasses
  objectClasses: ( 0.9.2342.19200300.100.4.19 NAME 'simpleSecurityObject' DESC '
   Standard LDAP objectClass' SUP (ndsLoginProperties $ top) STRUCTURAL )
  ```

10.1.3 Schritt 3: LDIF-Datei importieren

Importieren Sie mit folgendem NetIQ Import Conversion Export (ICE)-Befehl die veränderte Schemavergleichs-LDIF-Datei (in unserem Beispiel `err.ldf`):

```
ice -e error_file -SLDIF -f modified_LDIF_file -DLDAP -s eDirectory_server -p
eDirectory_port -d eDirectory_Admin_DN -w eDirectory_password
```

Beispiel:

```
ice -e errors.ldf -SLDIF -f err.ldf -DLDAP -s edir_srv2 -p edir_port2 -d
cn=admin,o=org -w pwd1
```

10.2 Migration von Active Directory Schema zu NetIQ eDirectory unter Verwendung von ICE

Bei der Schemamigration von Active Directory zu NetIQ eDirectory mittels ICE tritt für die Objektklasse `Computer` der Fehler `keine eindeutige Benennung (-651)` auf.

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

„Schritt 1: Aktualisierungsvorgang für Schema-Cache ausführen“, auf Seite 67
„Schritt 2: Fehlerhafte LDIF-Datei korrigieren, um die Fehler zu beseitigen“, auf Seite 67
„Schritt 3: LDIF-Datei importieren“, auf Seite 69

10.2.1 Schritt 1: Aktualisierungsvorgang für Schema-Cache ausführen

Stellen Sie bei der Schemamigration von Active Directory zu NetIQ eDirectory mittels ICE sicher, dass für ICE die Fehlerprotokolloption (`-e`) wie folgt festgelegt wird:

```
ice -e error_file -S ldap -s Active_Directory_server -p Active_Directory_port -d
Active_Directory_full_admin_context -w Active_Directory_password -D ldap -s
eDirectory_server -p eDirectory_port -d eDirectory_full_admin_context -w
eDirectory_password
```

Beispiel:

```
ice -e err.ldf -S ldap -s activesrv1 -p activeport1 -d cn=admin,o=company -w
activepwd -D ldap -s edirsrv2 -p edirport2 -d cn=admin,o=company -w edirpwd
```

10.2.2 Schritt 2: Fehlerhafte LDIF-Datei korrigieren, um die Fehler zu beseitigen

Der fehlerhafte Eintrag würde wie folgt in der Datei `err.ldf` vorhanden sein:

```
dn: cn=schema

changetype: modify

delete: objectclasses

objectclasses: ( 2.16.840.1.113719.1.1.6.1.4 NAME 'computer' )

-

add: objectclasses

objectclasses: ( 2.16.840.1.113719.1.1.6.1.4 NAME 'computer' SUP (device $
 user ) STRUCTURAL MAY (operator $ server $ status $ cn $ networkAddress $
 local PolicyFlags $ defaultLocalPolicyObject $ machineRole $ location $
 netbootInitialization $ netbootGUID $ netbootMachineFilePath $ siteGUID $
 operatingSystem $ operatingSystemVersion $ operatingSystemServicePack $
 operatingSystemHotfix $ volumeCount $ physicalLocationObject $ dNSHostName
 $ policyReplicationFlags $ managedBy $ rIDSetReferences $ catalogs $
 netbootSIFFile $ netboot MirrorDataFile ) X-NDS_NOT_CONTAINER '1' X
 -NDS_NONREMOVABLE '1' X-NDS_NAME 'Computer' )

-
```

Bearbeiten Sie diesen Eintrag in der Fehlerdatei (in diesem Beispiel `err.ldf`) so, dass die Objektklasse `user` wie unten dargestellt von der Liste übergeordneter Objektklassen in der Definition der Objektklasse `Computer` entfernt wird:

```
dn: cn=schema

changetype: modify

delete: objectclasses

objectclasses: ( 2.16.840.1.113719.1.1.6.1.4 NAME 'computer' )

-

add: objectclasses

objectclasses: ( 2.16.840.1.113719.1.1.6.1.4 NAME 'computer' SUP device
 STRUCTURAL MAY (operator $ server $ status $ cn $ networkAddress $ local
 PolicyFlags $ defaultLocalPolicyObject $ machineRole $ location $
 netbootInitialization $ netbootGUID $ netbootMachineFilePath $ siteGUID $
 operatingSystem $ operatingSystemVersion $ operatingSystemServicePack $
 operatingSystemHotfix $ volumeCount $ physicalLocationObject $ dNSHostName
 $ policyReplicationFlags $ managedBy $ rIDSetReferences $ catalogs $
 netbootSIFFile $ netbootMirrorDataFile ) X-NDS_NOT_CONTAINER '1' X
 -NDS_NONREMOVABLE '1' X-NDS_NAME 'Computer' )

-
```

10.2.3 Schritt 3: LDIF-Datei importieren

Importieren Sie nun den bearbeiteten Eintrag mit dem folgenden ICE-Befehl:

```
ice -S ldif -f LDIF_file -D ldap -s Novell_eDirectory_server -p port_number -d
full_admin_context -w password
```

Beispiel:

```
ice -S ldif -f err.ldf -D ldap -s edirsrv1 -p edirport1 -d cn=admin,o=company -w
pwd1
```

10.3 Migration von OpenLDAP zu NetIQ eDirectory

10.3.1 Voraussetzungen

Die von einem OpenLDAP-Server migrierten Daten können MD5-Passwörter enthalten. Dies kann zum Anhalten der Anwendung führen, wenn die entsprechenden NetIQ Modular Authentication Service (NMAS)-Methoden nicht installiert sind. Die NMAS-Methode „Einfaches Passwort“ muss mit dem folgenden Befehl für NetIQ eDirectory installiert werden:

`nmasinst -addmethod` *`admin_context treename configfile`* `-h` *`Hostname:port`*`-w` *`password`*

Beispiel: `nmasinst -addmethod admin.novell eDir-Tree /Linux/eDirectory/nmas/ NmasMethods/Novell/SimplePassword/config.txt -h eDir_srv:524 -w secret`

10.3.2 Migration des OpenLDAP-Schemas zu eDirectory

Führen Sie folgende Schritte aus, um das OpenLDAP-Schema zu eDirectory zu migrieren:

- „Schritt 1: Aktualisierungsvorgang für Schema-Cache ausführen“, auf Seite 72
- „Schritt 2: Fehlerhafte LDIF-Datei korrigieren, um die Fehler zu beseitigen“, auf Seite 72

Schritt 1: Aktualisierungsvorgang für Schema-Cache ausführen

Mit folgendem Befehl können Sie die Fehler, die beim Vergleich des Schemas auftreten, in eine Fehlerdatei schreiben:

```
ice -e error_file -C -a -S ldap -s OpenLDAP_server -p Open_LDAP_port - D ldap -s
eDirectory_server -p eDirectory_port -d eDirectory_full_admin_context -w
eDirectory_password
```

Beispiel:

```
ice -e err.ldf -C -a -SLDAP -s open_srv1 -p open_port1 -DLDAP -s edir_srv2 -p
edir_port2 -d cn=admin,o=novell -w secret
```

Alle beim Vergleichen des Schemas aufgetretenen Fehler werden in die Fehlerdatei (in diesem Beispiel `err.ldf`) geschrieben.

Schritt 2: Fehlerhafte LDIF-Datei korrigieren, um die Fehler zu beseitigen

OpenLDAP definiert bestimmte Schemadefinitionen öffentlich, unter anderem die Attribute `objectClasses`, `attributeTypes`, `ldapSyntaxes` und `subschemSubentry`. Diese Definitionen existieren intern sind für das Schema von wesentlicher Bedeutung. Sie können daher nicht geändert werden. Vorgänge, die versuchen, diese Definitionen zu ändern, verursachen folgenden Fehler:

```
LDAP error : 53 (DSA is unwilling to perform)
```

Datensätze, die Bezüge zu diesen Definitionen enthalten, verursachen folgenden Fehler:

```
LDAP error : 16 ( No such attribute )
```

Datensätze, die einen Bezug zu diesen Objekten enthalten oder versuchen, diese Definitionen zu ändern, müssen in der LDIF-Fehlerdatei (in diesem Beispiel `err.ldf`) kommentiert werden.

10.3.3 Migration der OpenLDAP-Daten zu NetIQ eDirectory

Führen Sie folgenden Befehl aus, um die Daten zu migrieren:

```
ice -e error_data.ldif -SLDAP -s OpenLDAP_server -p OpenLDAP_port  -d admin_context
-w password -t -b dc=blr,dc=novell,dc=com -F objectclass=* -DLDAP -d  admin_context
-w password  -l  -F
```

Beispiel:

```
ice -e err_data.ldif -SLDAP -s open_srv1 -p open_port1  -d
cn=administrator,dc=blr,dc=novell,dc=com -w secret1 -t -b dc=blr,dc=novell,dc=com
-F objectclass=* -DLDAP -d cn=admin,o=novell -w secret2 -l -F
```

Bei einigen Objekten können auch aufgrund von Vorverweisen oder internen Abhängigkeiten zu Objekten Fehler auftreten, die möglicherweise keine Anwendung anhalten.

10.3.4 PAM nach der Migration mit NetIQ eDirectory funktionsfähig machen

Nach der Migration von OpenLDAP zu eDirectory sind einige Änderungen erforderlich, damit PAM mit eDirectory verwendet werden kann.

Änderungen in der Datei „/etc/ldap.conf“

```
# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously.
  binddn cn=admin,o=acme
  ...
# The credentials to bind with.
# Optional: default is no credential.
  bindpw secret
  ...
# The search scope.
  scope sub
  ...
# Filter to AND with uid=%s
  pam_filter objectclass=inetorgperson
  ...
# Remove old password first, then update in
# cleartext. Necessary for use with Novell
# Directory Services (NDS)
  pam_password nds
  ...
  ssl off
  ...
```

Änderungen an den Daten im Verzeichnis

Diese Änderung betrifft nur Szenarien, in denen die Benutzerobjekte in OpenLDAP den Passwort-Hash-Algorithmus CRYPT verwenden.

Fügen Sie mit iManager folgendes Attribut mit dem angegebenen Wert zum Container hinzu, der die Benutzerobjekte enthält:

Attribut: `sasDefaultLoginSequence`

Wert: einfaches Passwort

11 Schema

Dieser Abschnitt enthält Informationen zur Behebung von Schemafehlern.

Behebung von Schemafehlern

Wenn die Verknüpfung einer Zusatzklasse zu einem Objekt aufgehoben wird, wird der Wert nicht sofort gelöscht, sondern zunächst als „nicht vorhanden“ gekennzeichnet. Die Zusatzklasse wird mit dem Eintrag verknüpft, bis der DRL-Vorgang die Werte bei der tatsächlichen Objektvalidierung bereinigt.

Da DRL ein ressourcenintensiver Hintergrundprozess ist, werden andere Vorgänge während der Bereinigung langsamer ausgeführt. Die Dauer des Bereinigungsvorgangs hängt von der Anzahl der tatsächlichen Objekte und der externen Referenzen im System ab. Da der Vorgang den Prozessor und den Arbeitsspeicher stark beansprucht, sollte er nicht zu häufig ausgeführt werden. Standardmäßig wird der Backlinker-Hintergrundvorgang 50 Minuten nach dem Starten von „ndsd“ und dann alle 13 Stunden ausgeführt.

Das Löschen einer Zusatzklasse von einem Eintrag kann 0 bis 13 Stunden in Anspruch nehmen, zusätzlich der erforderlichen Zeit zur Verarbeitung des Eintrags im System.

Um das Problem zu umgehen, löschen Sie den Eintrag der Zusatzklasse, indem Sie den Backlinker-Vorgang über DSTrace oder iMonitor auslösen.

HINWEIS: Wenn das Objekt gelöscht wird, werden die Werte sofort getilgt, weil der Löschvorgang von anderen Hintergrundvorgängen verarbeitet wird.

---

12 DSRepair

12.1 Ausführen von DSRepair auf einer NFS-gemounteten DIB unter Linux

Unter Umständen treten die Fehler -732 oder -6009 auf, wenn Sie ndsrepair-Operationen (DSRepair) auf einer NFS-gemounteten DIB auf Linux-Systemen ausführen.

12.2 DSRepair bleibt bei Ausführung mit Option -R hängen

Wenn die Attributverschlüsselung für indizierte Attribute aktiviert ist, bleibt ndsrepair (DSRepair) bei der Ausführung mit der Option `-R` hängen.

12.3 Ausführen von DSRepair nach einer Aufrüstung oder Migration

Wenn „DSRepair“ nach dem Aufrüsten oder Migrieren eines 8.7.3.x-Servers unbeaufsichtigt ausgeführt wird, wird die Fehlermeldung `Invalid Ancestor ID list for the entry` („Ungültige IDs der übergeordneten Knoten“) angezeigt.

Dies kann ignoriert werden, da eine Aufrüstung der ID des übergeordneten Knotens nach Abschluss der DIB-Aufrüstung bzw. -Migration als Teil des Hintergrundvorgangs vorgenommen wird.

13 Reproduktion

eDirectory bietet den widerstandsfähigen Verzeichnisdienst von NetIQ sowie die Fehlertoleranz, die Bestandteil der Reproduktion ist. Durch Reproduktion können Sie Kopien der eDirectory-Datenbank, oder von Teilen davon, auf mehreren Servern gleichzeitig speichern.

13.1 Probleme bei der verschlüsselten Reproduktion

13.1.1 Konfigurieren der verschlüsselten Reproduktion über iManager

Die verschlüsselte Reproduktion kann nicht über iManager konfiguriert werden, wenn einer der Server im Reproduktionsring abgeschaltet ist.

13.1.2 Zusammenführen von Bäumen mit verschlüsselter Reproduktion nicht möglich

Wenn die verschlüsselte Reproduktion aktiviert ist, ist das Zusammenführen von Bäumen nicht möglich. Deaktivieren Sie die sichere Reproduktion auf jedem Baum, bevor Sie eine Zusammenführung vornehmen.

13.2 Probleme mit der eDirectory-Reproduktion beheben

Sie sollten immer mehrere Reproduktionen von eDirectory-Partitionen erstellen. Wenn eine Reproduktion beschädigt wird oder aufgrund einer fehlerhaften Festplatte verloren geht, können Sie diese Reproduktion so mithilfe von ConsoleOne oder NetIQ iManager löschen und durch eine neue Kopie der intakten Reproduktion ersetzen.

Weitere Informationen über das Löschen von Reproduktionen finden Sie unter „Verwalten von Reproduktionen“ (http://www.novell.com/documentation/edir88/edir88/data/fbgciaad.html) im *NetIQ eDirectory 8.8 SP8-Administrationshandbuch*.

14 Probleme beim Klonen von DIB

14.1 DIB kann nicht geklont werden - Fehler -601 und -603

Wenn verschlüsselte Attribute und die verschlüsselte Reproduktion auf Baumebene aktiviert sind, ist das Klonen von DIB nicht möglich und folgende Fehler werden angezeigt:

- Klonen von DIB auf den Zielserver ist während der Konfiguration von SAS nicht möglich; Fehler -601
- Nach dem Klonen von DIB schlägt das neu erstellte Klonobjekt fehl; Fehler -603

Diese Probleme lassen sich umgehen, indem Sie die verschlüsselten Attribute und die verschlüsselte Reproduktion deaktivieren.

14.2 DIB kann möglicherweise nach der Offlineverarbeitung sehr großer Datenmengen nicht sofort geklont werden

Wenn Sie unmittelbar nach dem Offline-Bulkload einen Server klonen, tritt möglicherweise ein Fehler auf, wenn bei der Datenverarbeitung die Option „disable indices“ (Indizes deaktivieren) aktiviert war.

Dies ist jedoch kein Problem, wenn der DIB-Klon ein paar Stunden nach der Bulkload-Operation gestartet wird.

14.3 Problem beim Klonen, wenn verschlüsselte Reproduktion aktiviert ist

Wenn während des Klonens auf dem Quellserver die verschlüsselte Reproduktion aktiviert ist, müssen Sie den geklonten Server in der Richtlinie für die Reproduktionsverschlüsselung vorübergehend ausschließen. Nach Abschluss der Konfiguration des geklonten Servers können Sie diese Einstellung wieder ändern.

15 NetIQ PKI (Public Key Infrastructure; Infrastruktur für öffentliche Schlüssel)

15.1 Nicht funktionierende PKI-Vorgänge

Wenn PKI-Vorgänge in ConsoleOne oder iManager nicht funktionieren, kann dies darauf zurückzuführen sein, dass die NetIQ PKI-Services unter Linux nicht ausgeführt werden. Starten Sie die PKI-Services durch Eingabe des Befehls `npki -1`.

Wenn Sie keine Zertifikate erstellen können, müssen Sie sicher stellen, dass das NICI-Modul ordnungsgemäß installiert wurde. Siehe „Initialisierung des NICI-Moduls auf dem Server“ im *NetIQ eDirectory 8.8 SP8-Administrationshandbuch*. Informationen zur Überprüfung der Initialisierung von NICI finden Sie unter „Überprüfen, ob NICI auf dem Server installiert und initialisiert ist“ im *NetIQ eDirectory 8.8 SP8-Administrationshandbuch*.

15.2 Wenn die Konfiguration eines eDirectory-Servers, der in einem Baum mit mehreren Servern als Baumschlüsselserver fungiert, entfernt wird, nachdem die vorhandenen eDirectory-Objekte zu einem anderen Server verschoben wurden, tritt ein Fehler mit der Fehlerbeschreibung „Entscheidend wichtige Reproduktion“ auf.

Um den Vorgang abzuschließen, ändern Sie das Attribut der Schlüsselserver-DN im W0-Objekt unter „Sicherheitscontainer“ > „KAP“ in einen anderen Server im Baum, der den Baumschlüssel von diesem Server heruntergeladen hat.

1. Klicken Sie in NetIQ iManager auf die Schaltfläche *Rollen und Aufgaben* .
2. Klicken Sie auf *eDirectory-Verwaltung* > *Objekt bearbeiten*.

3 Geben Sie den Namen und den Kontext des W0-Objekts (üblicherweise „W0.KAP.Security“) an und klicken Sie auf *OK*.

4 Wählen Sie in der Spalte *Gewertete Attribute* den Eintrag *NDSPKI:SD Key Server DN* aus und klicken Sie auf *Bearbeiten*.

5 Geben Sie den Namen und den Kontext eines anderen Servers im Feld *Security Domain Key Server's DN* (DN des Schlüsselservers der Sicherheitsdomäne) an und klicken Sie auf *OK*.

6 Klicken Sie auf *Anwenden* und dann auf *OK*.

15.3 Bei der Deinstallation des eDirectory-Servers, der die Zertifizierungsstelle enthält, werden die auf diesem Server erstellten KMOs zu einem anderen Server im Baum verschoben und werden dadurch ungültig

Erstellen Sie die Zertifizierungsstelle und die KMOs für den Baum neu. Weitere Informationen finden Sie unter „Erstellen eines organisationalen Zertifizierungsstellenobjekts“ und „Erstellen eines Serverzertifikatsobjekts“ im *NetIQ eDirectory 8.8 SP8-Administrationshandbuch*.

Es wird empfohlen, den eDirectory-Server, auf dem die Zertifizierungsstelle für den Baum erstellt wurde, nicht zu deinstallieren.

16 Behebung von Fehlern mit Dienstprogrammen unter Linux

16.1 Novell Import Convert Export-Programm

Wenn ein LDAP-Server aktualisiert oder entladen wird, während ein NetIQ Import Conversion Export-Vorgang ausgeführt wird, wird die Meldung `Zeitüberschreitung bei LBURP` auf dem Bildschirm angezeigt. Der Server wird später wiederhergestellt, wenn beim LBURP-Vorgang eine Zeitüberschreitung auftritt.

16.2 ndsconfig-Dienstprogramm

Dieser Abschnitt behandelt folgende Themen:

16.2.1 ndsconfig-Dienstprogramms zum Ausführen von einem nicht-standardmäßigen Standort konfigurieren

Wenn Sie das ndsconfig-Dienstprogramm von einem anderen Speicherort als dem Standardverzeichnis `/opt/novell/eDirectory/bin` ausführen und dabei ein Fehler auftritt, stellen Sie sicher, dass Sie „ndspath“ vor dem Ausführen von „ndsconfig“ exportieren. Verwenden Sie den folgenden Befehl:

```
source /opt/novell/eDirectory/bin/ndspath
```

Geben Sie nach dem Exportieren des Befehls `ndsconfig` anstelle von `./ndsconfig` ein, um das ndsconfig-Dienstprogramm auszuführen.

16.2.2 ndsconfig kann ungültigen Konfigurationsdateipfad nicht überprüfen

Zur Erstellung der erforderlichen Konfigurationsdatei benötigt ndsconfig den vollständigen Pfad und den Namen der Konfigurationsdatei. Wenn sowohl für die Konfigurationsdatei als auch für das Instanzverzeichnis die gleiche Pfadangabe übergeben wird, kann ndsconfig die Konfigurationsdatei nicht erstellen und bricht den Vorgang ab.

16.2.3 ndsconfig get gibt bei nicht englischen Zeichen unsinnige Zeichen aus

Der Befehl `ndsconfig get` gibt unter Linux für einige Parameter, die andere als englische Zeichen enthalten, ungültige Zeichen aus.

Dieses Problem können Sie umgehen, indem Sie den gewünschten Parameternamen wie folgt eingeben:

```
ndsconfig get <anzuzeigender_Parameter>
```

Eine Liste der Parameter finden Sie auf der Manpage `nds.conf`.

16.3 ndsmerge-Dienstprogramm

Die PKI-Server sind nach einem Zusammenführungsvorgang nicht aktiv. Sie müssen mit dem Befehl `npki -l` neu gestartet werden.

Zusammenführungsvorgänge sind bei verschiedenen Versionen des Produkts unter Umständen nicht erfolgreich. Wenn auf dem Server eine ältere Version von NDS oder eDirectory ausgeführt wird, führen Sie eine Aktualisierung auf die neueste Version von eDirectory aus und setzen Sie dann die Zusammenführungsvorgänge fort.

Das Zusammenführen von zwei Bäumen ist nicht erfolgreich, wenn einem Baum untergeordnete Container mit dem gleichen Namen sowohl im Ursprungs- als auch im Quellbaum vorhanden sind. Benennen Sie einen der Container um und setzen Sie dann den Zusammenführungsvorgang fort.

Beim Hinzufügungsvorgang kann die Fehlermeldung `-611 Unzulässige Beinhaltung` angezeigt werden. Bearbeiten Sie das Schema, indem Sie `ndsrepair` ausführen. Führen Sie dann `ndsrepair -S` aus und wählen Sie *Optionale Schemaerweiterungen* aus.

16.4 DSTrace-Dienstprogramm

Wenn Sie den DSTrace-Bildschirm einschalten, kann eine Fehlermeldung angezeigt werden, die darauf hinweist, dass ein primäres Objekt für die Bezugsverknüpfung ungültig ist. Wenn eDirectory ordnungsgemäß funktioniert, können Sie diese Meldung ignorieren.

16.5 ndsbackup-Dienstprogramm

Beim Sichern von eDirectory kann die Meldung `NDS Error: Connect to NDS server failed` (NDS-Fehler: Fehler bei der Verbindung zum NDS-Server) angezeigt werden. Eine mögliche Ursache ist, dass eDirectory einen anderen Port als den Standardport 524 überwacht. Geben Sie in der Befehlszeile die Portnummer ein, mit der eDirectory konfiguriert wurde. Wenn eDirectory beispielsweise mit Portnummer 1524 konfiguriert wurde, geben Sie Folgendes ein:

```
ndsbackup sR 164.99.148.82:1524
```

Beim Sichern von Daten in eDirectory 8.8 und höheren Versionen kann die Meldung „NDS Error: Requires a Password“ (NDS-Fehler: Passwort erforderlich) angezeigt werden. Dies kann daran liegen, dass der Server über Attribute verfügt, die zur Verschlüsselung gekennzeichnet sind, und Sie nicht die Option -E zum Verschlüsseln bzw. Entschlüsseln der Sicherungsdaten verwendet haben.

16.6 Verwenden von DSRepair

Dieser Abschnitt behandelt folgende Themen:

- „Syntax“, auf Seite 87
- Abschnitt 16.6.2, „Behebung von Fehlern mit DSRepair“, auf Seite 94

Durch Verwendung des Dienstprogramms DSRepair an der Serverkonsole ist Folgendes möglich:

- Probleme mit eDirectory beheben, z. B. falsche Datensätze, nicht übereinstimmende Schemas, falsche Serveradressen und externe Referenzen.
- Erweiterte Änderungen am eDirectory-Schema vornehmen.
- Die folgenden Operationen an der eDirectory-Datenbank ausführen:
  - Die Struktur der Datenbank automatisch, ohne Schließen der Datenbank und ohne Benutzerinteraktion prüfen.
  - Eine Datenbankindex-Prüfung durchführen.
  - Die Datenbank reparieren, ohne dass die Datenbank geschlossen wird oder Benutzer abgemeldet werden müssen.
  - Freien Speicherplatz zurückgewinnen, indem leere Datensätze entfernt werden.

16.6.1 Syntax

Zum Ausführen von DSRepair verwenden Sie folgende Syntax:

```
ndsrepair {-U| -P| -S| -C| -E| -N| -T| -J entry_id}
[-A yes|no] [-O yes|no] [-F filename] [-Ad]
```

Alternativ:

```
ndsrepair -R [-l yes|no [-u yes|no] [-m yes|no] [-i yes|no] [-f yes|no] [-d yes|no]
[-t yes|no] [-o yes|no] [-r yes|no] [-v yes|no] [-c yes|no] [-A yes|no] [-O yes|no]
[-F filename]
```

WICHTIG: Die Option `-Ad` sollte nicht ohne vorherige Anweisung vom technischen Support von NetIQ verwendet werden.

DSRepair-Optionen

Option	Beschreibung
-R	Repariert die lokale eDirectory-Datenbank. Mit dieser Reparaturoperation können Sie Inkonsistenzen in der lokalen Datenbank auflösen, damit sie von eDirectory geöffnet werden kann und der Zugriff ermöglicht wird. Diese Option weist untergeordnete Optionen auf, die Reparaturoperationen für die Datenbank erleichtern. Die mit der Option verwendeten Funktionsparameter sind unter „Mit der Option "-R" verwendete Funktionsparameter“, auf Seite 89 beschrieben. Diese Option ohne Unteroptionen stellt die empfohlene Reparaturmethode dar, sofern der NetIQ Support Sie nicht dazu auffordert, bestimmte Vorgänge manuell auszuführen.
-P	Option "Reproduktions- und Partitionsoperationen". Listet die Partitionen auf, die Reproduktionen in den eDirectory-Datenbankdateien des aktuellen Servers gespeichert haben. Das Menü „Reproduktionsoptionen“ enthält Optionen zum Reparieren von Reproduktionen, Abbrechen einer Partitionsoperation, Planen der Synchronisierung und zum Festlegen der lokalen Reproduktion als Masterreproduktion. Weitere Informationen finden Sie unter „Die Option "Reproduktions- und Partitionsoperationen"“, auf Seite 90.
-S	Option "Globale Schema-Operationen". Diese Option umfasst mehrere Schema-Operationen, die unter Umständen benötigt werden, um das Schema des Servers in Übereinstimmung mit der Masterreproduktion des Baumobjekts zu bringen. Die Operationen sollten jedoch nur verwendet werden, wenn unbedingt erforderlich. Die lokalen und unbeaufsichtigten Reparaturoperationen überprüfen bereits das Schema.
-C	Zum Ausführen der Option "Externe Referenzen prüfen". Dieser Befehl überprüft jedes einzelne externe Referenzobjekt, um festzustellen, ob eine Reproduktion gefunden werden kann, die das Objekt enthält. Wenn auf keinen Server zugegriffen werden kann, der eine Reproduktion der Partition enthält, in der sich das Objekt befindet, wird das Objekt nicht gefunden. Wenn das Objekt nicht gefunden werden kann, wird eine Warnmeldung ausgegeben.
-E	Option zum Melden der Reproduktionssynchronisierung. Dieser Befehl meldet den Synchronisierungsstatus der Reproduktion für alle Partitionen, die eine Reproduktion auf dem aktuellen Server besitzen. Diese Operation liest das Attribut „Synchronisierungsstatus“ aus dem Baumobjekt der Reproduktion auf jedem Server, der Reproduktionen der Partitionen enthält. Es werden die Uhrzeit der letzten ordnungsgemäßen Synchronisierung auf allen Servern sowie alle Fehler angezeigt, die seit der letzten Synchronisierung aufgetreten sind. Eine Warnmeldung wird angezeigt, wenn die Synchronisierung nicht innerhalb von 12 Stunden abgeschlossen wurde.
-N	Option "Dieser Datenbank bekannte Server". Listet alle Server auf, die der lokalen eDirectory-Datenbank bekannt sind. Wenn Ihr aktueller Server eine Reproduktion der Baumpartition enthält, zeigt dieser Server eine Liste aller Server im eDirectory-Baum an. Wählen Sie einen Server aus, um die Serveroptionen auszuführen.

Option	Beschreibung
-J	Repariert ein einzelnes Objekt auf dem lokalen Server. Sie müssen die Eintrags-ID (im hexadezimalen Format) des Objekts angeben, das Sie reparieren möchten. Diese Option können Sie anstelle der Option "Unbeaufsichtigte Reparatur" (-U) verwenden, wenn nur ein einzelnes beschädigtes Objekt repariert werden soll. Die Option „Unbeaufsichtigte Reparatur“ kann je nach der Größe der Datenbank mehrere Stunden in Anspruch nehmen. Mit dieser Option können Sie Zeit sparen.
-T	Option "Zeitsynchronisierung". Spricht alle Server an, die der lokalen eDirectory-Datenbank bekannt sind, und fragt bei jedem Server Informationen zum Zeitsynchronisierungsstatus ab. Wenn dieser Server eine Reproduktion der Baumpartition enthält, wird jeder Server im eDirectory-Baum abgefragt. Die Version von eDirectory, die auf jedem Server ausgeführt wird, wird ebenfalls angegeben.
-A	Zum Ausführen der Option "An vorhandene Datei anfügen". Die Informationen werden an die vorhandene Protokolldatei angefügt. Standardmäßig ist diese Option aktiviert.
-O	Zum Protokollieren der Ausgabe in einer Datei. Standardmäßig ist diese Option aktiviert.
-F *dateiname*	Protokolliert die Ausgabe in der angegebenen Datei.
-U	Option für unbeaufsichtigte vollständige Reparatur. DSRepair wird ohne Einwirkung des Benutzers ausgeführt und beendet. Mit dieser Option wird die Datenbank gesperrt und die Serververweisadressen aktualisiert. Sie können die Protokolldatei nach Abschluss der Reparatur anzeigen, um festzustellen, welche Aktionen von DSRepair ausgeführt wurden.

Mit der Option "-R" verwendete Funktionsparameter

Bearbeiter	Beschreibung
-l	Die eDirectory-Datenbank während der Reparatur sperren.
-u	Während der Reparatur temporäre eDirectory-Datenbank verwenden.
-m	Die ursprüngliche, nicht reparierte Datenbank beibehalten.
-i	Die eDirectory-Datenbankstruktur und den Index überprüfen.
-f	Freien Datenbankspeicher zurückgewinnen.
-d	Gesamte Datenbank neu aufbauen.
-t	Baumstruktur prüfen. Wählen Sie "Ja", um alle Baumstrukturverknüpfungen auf ordnungsgemäße Konnektivität in der Datenbank zu überprüfen. Wählen Sie "Nein", um die Überprüfung zu überspringen. Standard=Yes (Ja)
-o	Operationsschema neu erstellen.
-r	Alle lokalen Reproduktionen reparieren.
-v	Datenstromdateien prüfen.
-c	Lokale Referenzen überprüfen.

Globale Schema-Operationen

Mit der Option `ndsrepair -S ([-Ad] erweiterter Schalter)` können Sie eine Liste aller ausführbaren Schema-Operationen anzeigen. Die folgende Tabelle zeigt die verfügbaren Optionen:

Option	Beschreibung
Schema vom Masterserver anfordern	Fordert die Masterreproduktion des Stammverzeichnisses des Baums auf, ihr Schema mit diesem Server zu synchronisieren. Alle Änderungen, die am Schema vorgenommen werden, werden aus der Masterreproduktion des Baumobjekts für die nächsten 24 Stunden an diesen Server weitergeleitet. Wenn alle Server das Schema aus der Masterreproduktion anfordern, kann der Netzwerkverkehr zunehmen.
Lokales Schema zurücksetzen	Bewirkt eine Rücksetzung des Schemas, die die Zeitstempel im lokalen Schema löscht und eine eingehende Schemasynchronisierung anfordert. Diese Option ist bei Ausführung von der Masterreproduktion der Baumpartition aus nicht verfügbar. Dadurch wird verhindert, dass alle Server im Baum gleichzeitig zurückgesetzt werden.
Optionale Schemaerweiterungen	Erweitert und ändert das Schema für Beinhaltungserweiterung und andere Schemaerweiterungen. Die Option erfordert, dass dieser Server eine Reproduktion der Baumpartition enthält und dass die Reproduktion eingeschaltet ist.
Remote Schema importieren (Erweiterte Verbindungsoption)	Wählen Sie einen eDirectory-Baum aus, der das Schema enthält, das Sie zum Schema des aktuellen Baums hinzufügen möchten. Nachdem Sie einen Baum ausgewählt haben, wird die Verbindung zu dem Server hergestellt, der die Masterreproduktion der Baumpartition enthält. Das Schema dieses Servers wird verwendet, um das Schema des aktuellen Baums zu erweitern.
Befehl "Eine neue Epoche erklären" (Erweiterte Verbindungsoption)	Wenn Sie eine neue Schema-Epoche erklären, wird eine Verbindung zur Masterreproduktion der Baumpartition hergestellt, und unzulässige Zeitstempel werden in dem auf diesem Server deklarierten Schema repariert. Alle anderen Server erhalten eine neue Kopie des Schemas, einschließlich der reparierten Zeitstempel. Wenn der empfangende Server ein Schema enthält, das nicht in der neuen Epoche enthalten war, werden Objekte und Attribute, die das alte Schema verwenden, in die Objektklasse bzw. das Attribut „Unbekannt" geändert.

Die Option "Reproduktions- und Partitionsoperationen"

Mit dem folgenden Befehl können Sie Informationen zu jeder auf dem Server gespeicherten Reproduktion anzeigen:

```
ndsrepair -P
```

Markieren Sie die erforderliche Reproduktion. Die folgenden Optionen werden angezeigt:

- Alle Reproduktionen reparieren

Repariert alle Reproduktionen, die in der Reproduktionstabelle angezeigt werden.

- Markierte Reproduktion reparieren

  Repariert nur die markierte Reproduktion, die in der Reproduktionstabelle aufgelistet wird.

WICHTIG: Die Reparatur einer Reproduktion besteht im Überprüfen der einzelnen Objekte der Reproduktion auf Konsistenz mit dem Schema und im Überprüfen der Daten gemäß der Attributsyntax. Andere interne Datenstrukturen der Reproduktion werden ebenfalls überprüft. Wenn Sie die lokale eDirectory-Datenbank nicht innerhalb der letzten 30 Minuten repariert haben, sollten Sie dies nachholen, bevor Sie Reproduktionen reparieren.

- Sofortige Synchronisierung planen

  Mit dieser Option können Sie die sofortige Synchronisierung aller Reproduktionen planen. Diese Option ist sinnvoll, wenn Sie den DSTrace-Bildschirm anzeigen und eDirectory-Informationen aus dem Synchronisierungsvorgang anzeigen möchten, ohne zu warten, bis er gemäß dem normalen Zeitplan ausgeführt wird.

- Partitionsoperation abbrechen

  Dieser Befehl bricht eine Partitionsoperation auf der ausgewählten Partition ab. Diese Option kann unter Umständen erforderlich sein, wenn eine Operation nicht abgeschlossen werden kann oder aufgrund von Problemen im eDirectory-Baum nicht abgeschlossen wird, z. B. aufgrund eines fehlenden Servers oder schlechter Kommunikationsverbindungen. Einige Operationen können unter Umständen nicht abgebrochen werden, wenn Sie bereits zu weit fortgeschritten sind.

- Diesen Server als neue Masterreproduktion definieren

  Legt die lokale Reproduktion der ausgewählten Partition als neue Masterreproduktion fest. Verwenden Sie diese Option, um eine neue Masterreproduktion anzugeben, wenn die ursprüngliche Masterreproduktion verlorengegangen ist.

- Synchronisierungsstatus aller Server melden

  Meldet den Reproduktions-Synchronisierungsstatus aller Partitionen auf dem aktuellen Server. Es werden die Uhrzeit der letzten ordnungsgemäßen Synchronisierung auf allen Servern sowie alle Fehler angezeigt, die seit der letzten Synchronisierung aufgetreten sind.

- Die Reproduktionen auf allen Servern synchronisieren

  Ermittelt den vollständigen Synchronisierungsstatus auf jedem Server, der eine Reproduktion der ausgewählten Partition besitzt. Diese Option unterstützt Sie beim Beurteilen des Zustands einer Partition. Wenn alle Server mit einer Reproduktion der Partition einwandfrei synchronisiert sind, wird die Partition als einwandfrei betrachtet. Jeder Server wird sofort mit allen anderen Servern im Reproduktionsring synchronisiert. Server synchronisieren sich nicht selbst. Aus diesem Grund wird der Status der eigenen Reproduktionen des aktuellen Servers als Host angezeigt.

- Ring reparieren, alle Reproduktionen

  Repariert den Reproduktionsring aller Reproduktionen, die in der Reproduktionstabelle angezeigt werden.

- Ring reparieren, markierte Reproduktion

  Repariert den Reproduktionsring der markierten Reproduktion, die in der Reproduktionstabelle aufgelistet wird.

WICHTIG: Die Reparatur eines Reproduktionsrings besteht im Überprüfen der Reproduktionsring-Informationen auf jedem Server, der eine Reproduktion einer gegebenen Partition enthält, und im Überprüfen der Fern-ID-Informationen. Wenn Sie die lokale

eDirectory-Datenbank nicht innerhalb der letzten 30 Minuten repariert haben, sollten Sie dies nachholen, bevor Sie alle oder ausgewählte Ringe reparieren. Sie können die lokale Datenbank mit der Option `-R` reparieren. Weitere Informationen finden Sie unter „-R“, auf Seite 88.

- Reproduktionsring anzeigen

  Zeigt eine Liste aller Server an, die eine Reproduktion der ausgewählten Partition enthalten. Diese Server werden als Reproduktionsring bezeichnet. Die Reproduktionsringliste zeigt Informationen zum Typ einer Reproduktion sowie den aktuellen Status jedes einzelnen Servers im Ring an. Wählen Sie nach der Anzeige des Reproduktionsrings einen Server aus, um die Serveroptionen anzuzeigen.

  Serveroptionen

  - Synchronisierungsstatus des ausgewählten Servers melden

    Informiert über den Reproduktions-Synchronisierungsstatus einer ausgewählten Partition, die eine Reproduktion auf einem ausgewählten Server besitzt. Diese Operation liest das Attribut "Synchronisierungsstatus" aus dem Stammobjekt der Reproduktion auf jedem Server, der Reproduktionen der Partitionen enthält. Es werden die Uhrzeit der letzten ordnungsgemäßen Synchronisierung auf allen Servern sowie alle Fehler angezeigt, die seit der letzten Synchronisierung aufgetreten sind. Diese Option zeigt eine Warnmeldung an, wenn die Synchronisierung nicht innerhalb von zwölf Stunden abgeschlossen wurde.

  - Die Reproduktion auf dem markierten Server synchronisieren

    Ermittelt den vollständigen Synchronisierungsstatus auf dem ausgewählten Server, der eine Reproduktion der ausgewählten Partition besitzt. Diese Option unterstützt Sie beim Beurteilen des Zustands einer Partition. Wenn der Server mit einer Reproduktion auf der Partition einwandfrei synchronisiert ist, wird die Partition als einwandfrei betrachtet. Der Server wird sofort mit allen anderen Servern im Reproduktionsring synchronisiert. Der Server synchronisiert sich nicht selbst. Aus diesem Grund wird der Status der eigenen Reproduktion des aktuellen Servers als Host angezeigt.

  - Alle Objekte an alle Reproduktionen im Ring senden

    Sendet alle Objekte vom ausgewählten Server im Reproduktionsring an alle anderen Server, die eine Reproduktion der Partition enthalten. Diese Operation kann zu umfangreichem Netzwerkverkehr führen. Mit dieser Option können Sie sicher stellen, dass die Reproduktion der ausgewählten Partition auf dem ausgewählten Server im Reproduktionsring mit allen anderen Servern im Reproduktionsring synchronisiert wird. Diese Operation kann nicht auf einem Server ausgeführt werden, der nur eine untergeordnete Referenzreproduktion der Partition enthält.

  - Alle Objekte von der Masterreproduktion in diese Reproduktion übernehmen

    Empfängt alle Objekte von der Masterreproduktion in die Reproduktion auf den ausgewählten Servern. Diese Operation kann zu umfangreichem Netzwerkverkehr führen. Verwenden Sie diese Option um sicherzustellen, dass die Reproduktion der ausgewählten Partition auf dem ausgewählten Server im Reproduktionsring mit der Masterreproduktion synchronisiert wird. Diese Operation kann nicht auf einem Server ausgeführt werden, der nur eine Masterreproduktion enthält.

  - Den ganzen Servernamen anzeigen

    Dient zur Anzeige des kompletten Servernamens, wenn der Servername zu lang ist, um ihn innerhalb der Servertabelle anzeigen zu können.

  - Diesen Server aus dem Reproduktionsring entfernen

    (Erweiterte Verbindungsoption.) Entfernt einen ausgewählten Server aus der ausgewählten Reproduktion, die auf dem aktuellen Server gespeichert ist. Wenn ein Server im Reproduktionsring angezeigt wird, jedoch nicht mehr Teil des eDirectory-Baums ist oder

keine Reproduktion der Partition enthält, löschen Sie das Serverobjekt mit iManager. Nachdem das Serverobjekt gelöscht wurde, sollte das Objekt nicht mehr im Reproduktionsring enthalten sein.

WARNUNG: Wenn Sie diese Operation falsch verwenden, können nicht mehr behebbare Schäden an der eDirectory-Datenbank auftreten. Verwenden Sie diese Option nur, wenn Sie von einem NetIQ-Mitarbeiter des technischen Supports dazu angewiesen werden.

- Vollständigen Partitionsnamen anzeigen

  Bestimmt den vollständigen eindeutigen Partitionsnamens, wenn der Partitionsname zu lang ist, um ihn innerhalb der Reproduktionstabelle anzeigen zu können.

- Zeitstempel reparieren und eine neue Epoche angeben

  (Erweiterter Schalter.) Dieser Befehl stellt einen neuen Bezugspunkt für die Masterreproduktion zur Verfügung, damit alle Aktualisierungen von Reproduktionen der ausgewählten Partition aktuell sind. Diese Operation wird immer mit der Masterreproduktion einer Partition durchgeführt. Die Masterreproduktion muss sich nicht in der lokalen Reproduktion auf diesem Server befinden. Objekte werden beim Erstellen oder Bearbeiten mit Zeitstempeln versehen, die eindeutig sein müssen. Alle Zeitstempel in einer Masterreproduktion werden untersucht. Wenn Zeitstempel vorhanden sind, deren Zeitangabe später als die aktuelle Netzwerkzeit ist, werden diese durch einen neuen Zeitstempel ersetzt.

- Die markierte Reproduktion auf diesem Server zerstören

  (Erweiterter Schalter.) Entfernt die ausgewählte Reproduktion von diesem Server. Die Verwendung dieser Option ist nicht empfehlenswert. Verwenden Sie diese Option nur, wenn alle anderen Dienstprogramme nicht in der Lage sind, die Reproduktion zu löschen.

- Unbekannte Blattobjekte löschen

  (Erweiterter Schalter.) Dieser Befehl löscht alle Objekte in der lokalen eDirectory-Datenbank, die zur Objektklasse „Unbekannt“ gehören und keine untergeordneten Objekte verwalten. Diese Option markiert Objekte des Typs "Unbekannt" für den Löschvorgang. Der Löschvorgang wird später mit anderen Reproduktionen im eDirectory-Baum synchronisiert.

  WARNUNG: Verwenden Sie diese Option nur, wenn die Objekte nicht mit ConsoleOne oder iManager bearbeitet oder gelöscht werden können.

Optionen für dieser Datenbank bekannte Server

Die folgenden Reparatur-Optionen stehen für Server zur Verfügung:

- Alle Netzwerkadressen reparieren

  Dieser Befehl überprüft die Netzwerkadresse für jeden Server in der lokalen eDirectory-Datenbank. Je nach verfügbarem Transportprotokoll wird mit dieser Option der SLP-Verzeichnisagent nach dem Namen jedes Servers durchsucht. Jede Adresse wird anschließend mit der Eigenschaft "Netzwerkadresse" des Serverobjekts und dem Adressdatensatz in jeder Eigenschaft "Reproduktion" jedes Baumobjekts der Partition verglichen. Wenn sich die Adressen unterscheiden, werden sie so aktualisiert, dass sie gleich sind.

- Netzwerkadresse des markierten Servers reparieren

  Überprüft die Netzwerkadresse auf einen bestimmten Server in den lokalen eDirectory-Datenbankdateien. Je nach den aktuell gebundenen Transportprotokollen wird mit dieser Option der SLP-Verzeichnisagent nach dem Namen des Servers durchsucht.

* Vollständigen Servernamen anzeigen

  Dient zur Anzeige des vollständigen Servernamens, wenn der Servername zu lang ist, um ihn innerhalb der Servertabelle anzeigen zu können. Diese Option ist gleich der Option -P. Weitere Informationen finden Sie unter „-P“, auf Seite 88.

Beispiele

Um eine unbeaufsichtigte Reparatur auszuführen und Ereignisse in der Datei `/root/ndsrepair.log` zu protokollieren, oder Ereignisse an eine bereits vorhandene Protokolldatei anzuhängen, geben Sie folgenden Befehl ein:

```
ndsrepair -U  -A no -F /root/ndsrepair.log
```

Um eine Liste aller globalen Schema-Operationen zusammen mit den erweiterten Optionen anzuzeigen, geben Sie folgenden Befehl ein:

```
ndsrepair -S -Ad
```

Um die Datenbank durch Erzwingen einer Datenbank-Sperre zu reparieren, geben Sie den folgenden Befehl ein:

```
ndsrepair -R -l yes
```

HINWEIS: Die Eingabe für den Befehl `ndsrepair` kann von einer Optionsdatei umgeleitet werden. Die Optionsdatei ist eine Textdatei, die Optionen und Unteroptionen für die Reproduktions- und Partitionsvorgänge enthalten kann, für die keine Authentifizierung am Server erforderlich ist. Alle Optionen und Unteroptionen sind jeweils durch einen Zeilenumbruch getrennt. Stellen Sie sicher, dass der Inhalt der Datei in der richtigen Reihenfolge vorliegt. Liegt der Inhalt nicht in der richtigen Reihenfolge vor, ist das Ergebnis nicht vorhersehbar.

16.6.2 Behebung von Fehlern mit DSRepair

Fehler -786 beim Ausführen von DSRepair

Zur Verwendung von DSRepair muss in der Partition des Computers, in der DSRepair ausgeführt wird, mindestens dreimal so viel freier Speicherplatz wie die Größe der DIB verfügbar sein.

16.7 Verwenden von DSTrace

Um das DSTrace-Dienstprogramm in einer Linux-Umgebung auszuführen, führen Sie folgenden Befehl in der Servereingabeaufforderung aus:

```
/opt/novell/eDirectory/bin/ndstrace
```

Die vollständige Syntax für den ndstrace-Befehl lautet:

```
ndstrace [-l|-u|-c "command1;......"|--version] [-h <local_interface:port>] [--
config-file <configuration_file_path>] [thrd <thread ID>] [svty <severity_level>]
[conn <connection_ID>]
```

Das DSTrace-Dienstprogramm besteht aus drei Hauptkomponenten:

* „Grundfunktionen“, auf Seite 95
* „Fehlersuchmeldungen“, auf Seite 96
* „Hintergrundprozesse“, auf Seite 98

16.7.1 Grundfunktionen

Die Grundfunktionen von DSTrace sind:

- Anzeigen interner eDirectory-Aktivitäts- und Fehlersuchmeldungen in Linux.
- Einleiten begrenzter Synchronisierungsprozesse.

Sie können das DSTrace-Dienstprogramm entweder im UI-Modus oder im Befehlszeilenmodus ausführen. Standardmäßig wird DSTrace im UI-Modus ausgeführt. Geben Sie folgenden Befehl in der Eingabeaufforderung des Servers ein, um DSTrace im UI-Modus zu starten:

```
/opt/novell/eDirectory/bin/ndstrace
```

Geben Sie folgenden Befehl in der Eingabeaufforderung des Servers ein, um DSTrace im Befehlszeilenmodus zu starten:

```
/opt/novell/eDirectory/bin/ndstrace -l
```

Zum Ausführen der Grundfunktionen von DSTrace geben Sie unter Verwendung der folgenden Syntax Befehle an der Eingabeaufforderung des Servers ein:

```
ndstrace command_option
```

Die folgende Tabelle listet die Befehlsoptionen auf, die Sie eingeben können.

Option	Beschreibung
ON	Aktiviert den eDirectory-Überwachungsbildschirm mit den grundlegenden Meldungen der Ablaufverfolgung.
OFF	Deaktiviert den Überwachungsbildschirm.
ALL	Startet den eDirectory-Überwachungsbildschirm und zeigt alle Meldungen der Ablaufverfolgung an.
AGENT	Aktiviert den eDirectory-Überwachungsbildschirm mit den Meldungen der Ablaufverfolgung, die mit den Flaggen ON, BACKLINK, DSAGENT, JANITOR, RESNAME und VCLIENT übereinstimmen.
DEBUG	Aktiviert einen vordefinierten Satz von Meldungen der Ablaufverfolgung, die üblicherweise bei der Fehlersuche verwendet werden. Die gesetzten Flaggen sind ON, BACKLINK, ERRORS, EMU, FRAGGER, INIT, INSPECTOR, JANITOR, LIMBER, MISC, PART, RECMAN, REPAIR, SCHEMA, SKULKER, STREAMS und VCLIENT.
NODEBUG	Der Überwachungsbildschirm bleibt zwar aktiviert, aber alle vorher festgelegten Fehlersuchmeldungen werden deaktiviert. Mit dieser Option werden die Meldungen der Befehlsoption ON beibehalten.

16.7.2 Fehlersuchmeldungen

Wenn der DSTrace-Bildschirm aktiviert ist, werden die Informationen auf der Grundlage mehrerer Standardfilter angezeigt. Wenn Sie mehr oder weniger als die Standardinformationen anzeigen möchten, können Sie die Filter mit den Flaggen für die Fehlersuchmeldungen bearbeiten. Mit den Fehlersuchmeldungen können Sie den Status von eDirectory bestimmen und überprüfen, ob alles ordnungsgemäß funktioniert.

Jeder eDirectory-Prozess verfügt über eine Reihe von Fehlersuchmeldungen. Zum Anzeigen der Fehlersuchmeldungen für einen bestimmten Prozess verwenden Sie ein Pluszeichen (+) sowie den Prozessnamen oder die Option. Zum Deaktivieren der Anzeige für einen Prozess verwenden Sie ein Minuszeichen (-) sowie den Prozessnamen oder die Option. Es folgen einige Beispiele:

Meldung	Beschreibung
`set ndstrace = +SYNC`	Aktiviert die Synchronisierungsmeldungen.
`set ndstrace = -SYNC`	Deaktiviert die Synchronisierungsmeldungen.
`set ndstrace = +SCHEMA`	Aktiviert die Schemameldungen.

Sie können die Flaggen für die Fehlersuchmeldungen auch mit den booleschen Operatoren „&" (UND) und „|" (ODER) kombinieren. Die Syntax für die Steuerung der Fehlersuchmeldungen an der Serverkonsole lautet wie folgt:

```
set ndstrace = <trace_flag> [parameter]
```

In der nachfolgenden Tabelle werden die Ablaufverfolgungsflaggen für die Fehlersuchmeldungen beschrieben. Sie können Abkürzungen für jede Ablaufverfolgungsflagge eingeben.

Ablaufverfolgungsflagge	Beschreibung
ABUF	Meldungen und Informationen in Bezug auf eingehende und ausgehende Paketpuffer, die Daten enthalten, die gleichzeitig mit oder als Antwort auf eine eDirectory-Anforderung empfangen werden.
ALOC	Meldungen mit Details zur Arbeitsspeicherzuordnung.
AREQ	Meldungen in Bezug auf eingehende Anforderungen von anderen Servern oder Clients.
AUTH	Meldungen und Fehlerberichte in Bezug auf die Authentifizierung.
BASE	Fehlersuchmeldungen auf der niedrigsten Fehlersuchebene.
BLNK	Backlink- und eingehende Nachrufmeldungen und Fehlerberichte.
CBUF	Meldungen in Bezug auf ausgehende DS-Clientanforderungen.
CHNG	Cache-Änderungsmeldungen.
COLL	Status- und Fehlerberichte, die die Aktualisierungsinformationen eines Objekts betreffen, wenn die Aktualisierung kürzlich empfangen wurde.
CONN	Meldungen mit Informationen über die Server, zu denen Ihr Server eine Verbindung aufzubauen versucht, und über Fehler und Zeitüberschreitungen, die einen Verbindungsaufbau möglicherweise verhindern.
DNS	Meldungen über die in eDirectory integrierten DNS-Serverprozesse.
DRLK	Meldungen bezüglich Distributed Reference Link.

Ablaufverfolgungsflagge	Beschreibung
DVRS	Meldungen zu DirXML®-treiberspezifischen Bereichen, die von eDirectory möglicherweise bearbeitet werden.
DXML	Meldungen mit Details zu DirXML-Ereignissen.
FRAG	Meldungen vom NCP™-Fragmentierungsprogramm, das eDirectory-Meldungen in Meldungen in NCP-Größe aufteilt.
IN	Meldungen zu eingehenden Anforderungen und Prozessen.
INIT	Meldungen in Bezug auf die Initialisierung von eDirectory.
INSP	Meldungen in Bezug auf die Integrität von Objekten in der lokalen Datenbank des Ursprungsservers. Das Verwenden dieser Flagge führt zu einer verstärkten Beanspruchung des Festplattenspeichers, Arbeitsspeichers und Prozessors des Servers. Diese Flagge darf nicht aktiviert bleiben, es sei denn, Objekte werden beschädigt.
JNTR	Meldungen zu folgenden Hintergrundprozessen: Janitor, Reproduktionssynchronisierung und allgemeine Aktualisierung.
LDAP	Meldungen in Bezug auf den LDAP-Server.
LMBR	Meldungen, die sich auf den Limber-Prozess beziehen.
LOCK	Meldungen in Bezug auf die Verwendung und Änderung der Sperren der lokalen Datenbank des Ursprungsservers.
LOST	Meldungen in Bezug auf verlorene Einträge.
MISC	Meldungen von verschiedenen Quellen in eDirectory.
MOVE	Meldungen bezüglich des Verschiebens von Partitionen oder Teilbäumen.
NCPE	Meldungen, die den Server zeigen, der die Anforderungen der NCP-Ebene empfängt.
NMON	Meldungen in Bezug auf iMonitor.
OBIT	Meldungen vom Nachrufvorgang.
PART	Meldungen in Bezug auf Partitionsvorgänge von Hintergrundprozessen und von der Anforderungsverarbeitung.
PURG	Meldungen über den Tilgungsvorgang.
RECM	Meldungen in Bezug auf die Manipulation der Datenbank des Ursprungsservers.
RSLV	Berichte in Bezug auf die Verarbeitung der Anforderungen zur Namensauflösung.
SADV	Meldungen in Bezug auf die Registrierung von Baumnamen und Partitionen mit dem Service Location Protocol (SLP).
SCMA	Meldungen in Bezug auf den Schemasynchronisierungsprozess.
SCMD	Meldungen, die Details zu den schemabezogenen Vorgängen enthalten. Sie enthalten Details über die Eingangs- und die Ausgangssynchronisierung.
SKLK	Meldungen in Bezug auf den Reproduktionssynchronisierungsprozess.
SPKT	Meldungen in Bezug auf Informationen der NCP-Serverebene von eDirectory.

Ablaufverfolgungsflagge	Beschreibung
STRM	Meldungen in Bezug auf die Verarbeitung von Attributen mit einer Stream-Syntax.
SYDL	Meldungen mit weiteren Details während des Reproduktionsprozesses.
SYNC	Meldungen über den Eingangssynchronisierungsverkehr (was vom Server empfangen wird).
TAGS	Zeigt die Tag-Zeichenkette an, die die Trace-Option identifiziert, die das Ereignis generiert hat (für alle Zeilen des Trace-Prozesses).
THRD	Meldungen, die anzeigen, wann Hintergrundprozesse (Threads) beginnen und enden.
TIME	Meldungen über die transitiven Vektoren, die während des Synchronisierungsvorgangs verwendet werden.
TVEC	Meldungen in Bezug auf folgende Attribute: „Synchronisieren bis“, „Reproduktion bis“, „transitiver Vektor“.
VCLN	Meldungen in Bezug auf die Erstellung oder das Löschen von Verbindungen zu anderen Servern.

Beim Verwenden der Fehlersuchmeldungen in DSTrace werden Sie bemerken, dass einige der Ablaufverfolgungsflaggen hilfreicher sind als andere. Eine der beim technischen Support von NetIQ beliebtesten DSTrace-Einstellungen ist eigentlich ein Direktaufruf:

```
set ndstrace = A81164B91
```

Diese Einstellung aktiviert eine Gruppe Fehlersuchmeldungen.

16.7.3 Hintergrundprozesse

Zusätzlich zu den Fehlersuchmeldungen, die Sie bei der Überprüfung des Status von eDirectory unterstützen, stehen Ihnen eine Reihe von Befehlen zur Verfügung, mit denen die Ausführung der eDirectory-Hintergrundprozesse ausgelöst wird. Wenn Sie die Ausführung der Hintergrundprozesse auslösen möchten, geben Sie vor dem Befehl einen Stern (*) ein. Beispiel:

```
set ndstrace = *H
```

Bei einigen Hintergrundprozessen können Sie auch den Status, die Zeitsteuerung sowie die Prozesssteuerung ändern. Zum Ändern dieser Werte müssen Sie vor dem Befehl ein Ausrufezeichen (!) eingeben und einen neuen Parameter oder Wert eingeben. Beispiel:

```
set ndstrace = !H 15 (parameter_value_in_minutes)
```

Die Syntax für jede Anweisung zur Steuerung der Hintergrundprozesse von eDirectory lautet wie folgt:

```
set ndstrace = <trace_flag> [parameter]
```

In der nachfolgenden Tabelle werden die Ablaufverfolgungsflaggen für die Hintergrundprozesse, eventuell erforderliche Parameter sowie der Prozess beschrieben, der in den Ablaufverfolgungsflaggen angezeigt wird.

Ablaufverfolgungsflagge	Parameter	Beschreibung
*A	Keine	Setzt den Cache-Speicher für Adressen auf dem Ursprungsserver zurück.
*AD	Keine	Deaktiviert den Cache-Speicher für Adressen auf dem Ursprungsserver.
*AE	Keine	Aktiviert den Cache-Speicher für Adressen auf dem Ursprungsserver.
*B	Keine	Plant den Backlink-Vorgang so, dass mit der Ausführung auf dem Ursprungsserver in einer Sekunde begonnen wird.
!B	Uhrzeit	Legt das Intervall für den Backlink-Vorgang in Minuten fest. Standardwert=1500 Minuten (25 Stunden) Bereich= 2 bis 10080 Minuten (168 Stunden)
*CT	Keine	Zeigt die Tabelle der ausgehenden Ursprungsserververbindungen und die aktuellen statistischen Informationen für diese Tabelle an. Diese Statistiken enthalten keine Informationen über die eingehenden Verbindungen von anderen Servern oder Clients zum Ursprungsserver.
*CTD	Keine	Zeigt im durch Komma getrennten Format die Tabelle der ausgehenden Ursprungsserververbindungen und die aktuellen statistischen Informationen für diese Tabelle an. Diese Statistiken enthalten keine Informationen über die eingehenden Verbindungen von anderen Servern oder Clients zum Ursprungsserver.
*D	Reproduktions-rootEntryID	Entfernt die angegebene lokale Eintrags-ID von der Liste „Alle Objekte senden“ des Ursprungsservers. Die Eintrags-ID muss ein Partitionsstammobjekt definieren, das spezifisch für die lokale Datenbank des Servers ist. Dieser Befehl wird in der Regel nur dann verwendet, wenn der Prozess „Alle Aktualisierungen senden“ unaufhörlich versucht, Aktualisierungen anzuzeigen, und dabei Fehler auftreten, weil ein Server nicht erreichbar ist.
!D	Uhrzeit	Legt das Intervall für Ein- und Ausgangssynchronisierungauf die angegebene Minutenzahl fest. Standardwert: 24 Minuten. Bereich=2 bis 10080 Minuten (168 Stunden)
!DI	Uhrzeit	Legt das Intervall für Eingangssynchronisierung auf die angegebene Minutenzahl fest. Standardwert=24 Minuten Bereich= 2 bis 10080 Minuten (168 Stunden)
!DO	Uhrzeit	Legt das Intervall für Ausgangssynchronisierungauf die angegebene Minutenzahl fest. Standardwert=24 Minuten Bereich= 2 bis 10080 Minuten (168 Stunden)
*E	Keine	Initialisiert den Eintrags-Cache des Ursprungsservers neu.

Ablaufverfolgungsflagge	Parameter	Beschreibung
!E	Keine	Plant die Ein- und Ausgangssynchronisierungsvorgänge, um mit der Ausführung zu beginnen.
!EI	Keine	Plant den Eingangssynchronisierungsvorgang, um mit der Ausführung zu beginnen.
!EO	Keine	Plant den ausgehenden Synchronisierungsvorgang, um mit der Ausführung zu beginnen.
*F	Keine	Plant den Prozess der allgemeinen Aktualisierung, der Teil des Janitor-Vorgangs ist, so, dass mit der Ausführung auf dem Ursprungsserver in fünf Sekunden begonnen wird.
!F	Uhrzeit	Legt das Intervall für die allgemeine Aktualisierung in Minuten fest. Standardwert=240 Minuten (4 Stunden) Bereich= 2 bis 10080 Minuten (168 Stunden)
*FL	1-10	Legt die Anzahl der von DSTrace verwendeten fortlaufenden Protokolldateien fest. Wenn für diesen Parameter ein Wert größer 1 festgelegt wird, benennt DSTrace die Datei `ndstrace.log` auf dem Ursprungsserver in `ndstrace1.log` um, sobald sie die konfigurierte maximale Dateigröße erreicht hat, und erstellt eine neue Datei `ndstrace.log`. Wenn diese neue Datei wiederum die maximale Dateigröße erreicht hat, wird die vorige Datei `ndstrace1.log` in `ndstrace2.log` umbenannt und die neuere Datei `ndstrace.log` wird in `ndstrace1.log` umbenannt. Dieser Prozess wird fortgeführt, bis DSTrace die mit dieser Option festgelegte maximale Anzahl fortlaufender Protokolldateien erreicht hat. Wenn die angegebene Grenze erreicht wird, werden die ältesten Protokolldateien gelöscht, sodass stets nur die festgelegte maximale Dateizahl beibehalten wird. Sie können maximal 10 fortlaufende Protokolldateien konfigurieren. Standardmäßig muss DSTrace mindestens 1 fortlaufende Protokolldatei verwenden. Wenn Sie den Parameter auf 0 setzen, verwendet DSTrace einen Parameterwert von 1.
*G	Reproduktions-rootEntryID	Baut den Änderungs-Cache der festgelegten Stammpartitions-ID neu auf.
*H	Keine	Plant den Vorgang der Reproduktionssynchronisierung so, dass mit der Ausführung auf dem Ursprungsserver sofort begonnen wird.
!H	Uhrzeit	Legt das Intervall in Minuten für den Heartbeat-Synchronisierungsvorgang fest. Standardwert=30 Minuten Bereich= 2 bis 1440 Minuten (24 Stunden)
*HR	Keine	Löscht den zuletzt gesendeten Vektor im Speicher.

Ablaufverfolg ungsflagge	Parameter	Beschreibung
*I	Reproduktions-rootEntryID	Fügt die angegebene lokale Eintrags-ID der Liste „Alle Objekte senden“ des Ursprungsservers hinzu. Die Eintrags-ID muss ein Partitionsstammobjekt definieren, das spezifisch für die lokale Datenbank des Servers ist. Der Reproduktionssynchronisierungs-Vorgang prüft die Liste "Alle Objekte senden". Wenn sich die Eintrags-ID eines Partitionsstammobjekts in der Liste befindet, synchronisiert eDirectory alle Objekte und Attribute in der Partition, unabhängig vom Wert des Attributs „Synchronisiert bis“.
!I	Uhrzeit	Legt das Intervall in Minuten für den Heartbeat-Synchronisierungsvorgang fest. Standardwert=30 Minuten Bereich= 2 bis 1440 Minuten (24 Stunden)
*J	Keine	Plant den Tilgungsprozess, der Teil des Reproduktionssynchronisierungsvorgangs ist, so, dass mit der Ausführung auf dem Ursprungsserver begonnen wird.
!J	Uhrzeit	Legt das Intervall für den Janitor-Vorgang in Minuten fest. Standardwert=2 Minuten Bereich=1 bis 10080 Minuten (168 Stunden)
*L	Keine	Plant den Limber-Vorgang so, dass mit der Ausführung auf dem Ursprungsserver in fünf Sekunden begonnen wird.
*M	Byte	Ändert die maximale Größe der Datei, die von der Datei `ndstrace.log` des Ursprungsservers verwendet wird. Der Befehl kann unabhängig vom Status der Fehlersuchdatei verwendet werden. Die festgelegten Byte müssen ein Dezimalwert zwischen 10000 Byte und 100 MB sein. Wenn der festgelegte Wert höher oder niedriger als der festgelegte Bereich ist, tritt keine Änderung ein.
!M	Keine	Gibt den maximal verfügbaren Arbeitsspeicher an, der von eDirectory verwendet wird.
!N	0|1	Legt die Namensform fest. 0=nur Hexadezimal 1=vollständige Dezimalform
*P	Keine	Zeigt die abstimmbaren Parameter und die jeweiligen Standardeinstellungen an.
*R	Keine	Setzt die Größe der Datei `ndstrace.log` auf null Byte zurück. Dieser Befehl entspricht dem Parameter SET beim Setzen der Länge der NDS-Ablaufverfolgungsdatei auf Null.
*S	Keine	Plant den Skulker-Prozess, bei dem überprüft wird, ob eine der Reproduktionen auf dem Server synchronisiert werden muss.
!SI	Uhrzeit	Legt das Intervall in Minuten für den eingehenden Schemasynchronisierungsvorgang fest. Standardwert=24 Minuten Bereich= 2 bis 10080 Minuten (168 Stunden)

Ablaufverfolgungsflagge	Parameter	Beschreibung
!SO	Uhrzeit	Legt das Intervall in Minuten für den ausgehenden Schemasynchronisierungsvorgang fest. Standardwert=24 Minuten Bereich= 2 bis 10080 Minuten (168 Stunden)
!SIO	Uhrzeit	Deaktiviert den eingehenden Schemasynchronisierungsvorgang für die festgelegte Minutenzahl. Standardwert=24 Minuten Bereich= 2 bis 10080 Minuten (168 Stunden)
!SO0	Uhrzeit	Deaktiviert den eingehenden Schemasynchronisierungsvorgang für die festgelegte Minutenzahl. Standardwert=24 Minuten Bereich= 2 bis 10080 Minuten (168 Stunden)
*SS	Keine	Aktiviert eine sofortige Schemasynchronisierung.
*SSA	Keine	Plant den Vorgang der Schemasynchronisierung so, dass er sofort begonnen wird, und erzwingt die Schemasynchronisierung mit allen Zielservern. Dies gilt auch dann, wenn sie in den letzten 24 Stunden synchronisiert wurden.
*SSD	Keine	Setzt die Schemasynchronisierungsliste des Ursprungsservers zurück. Diese Liste gibt an, mit welchen Servern der Ursprungsserver während des Vorgangs der Schemasynchronisierung synchronisiert werden soll. Ein Server, auf dem keine Reproduktionen gespeichert sind, sendet eine Anforderung, die in der Zielliste eines Servers einzuschließen ist, auf dem eine Reproduktion mit seinen Serverobjekten enthalten ist.
*SSL	Keine	Druckt die Liste der Schemasynchronisierungen von Zielservern.
*ST	Keine	Zeigt die Statusinformation für die Hintergrundvorgänge auf dem Ursprungsserver an.
*STX	Keine	Zeigt die Statusinformation für Backlink-Vorgänge (externe Referenzen) auf dem Ursprungsserver an.
*STS	Keine	Zeigt die Statusinformation für die Schemasynchronisierungsvorgänge auf dem Ursprungsserver an.
*STO	Keine	Zeigt die Statusinformation für Backlink-Vorgänge (Nachrufe) auf dem Ursprungsserver an.
*STL	Keine	Zeigt die Statusinformation für die Limber-Vorgänge auf dem Ursprungsserver an.
!T	Uhrzeit	Legt das Intervall in Minuten für die Prüfung des Serverstatus „Hochgefahren“ fest. Standardwert=30 Minuten Bereich=1 bis 720 Minuten (12 Stunden)

Ablaufverfolgungsflagge	Parameter	Beschreibung
*U	Optionale ID des Servers	Wenn der Befehl keine Eintrags-ID enthält, wird der Status jedes Servers, der zuvor als **heruntergefahren** gekennzeichnet wurde, auf **hochgefahren** geändert. Wenn der Befehl eine lokale Eintrags-ID enthält, wird der Status des angegebenen Servers von **Heruntergefahren** auf **Hochgefahren** geändert. Eintrags-IDs sind für die Datenbank des Ursprungsservers spezifisch und müssen sich auf ein Objekt beziehen, das einen Server darstellt.
!V	Eine Liste	Führt die beschränkten eDirectory-Versionen auf. Falls keine Versionen aufgeführt sind, gibt es keine Beschränkungen. Die Versionen werden durch Komma getrennt.
*Z	Keine	Zeigt die gegenwärtig geplanten Aufgaben an.

17 NMAS auf Linux

17.1 Anmeldung mit keiner Methode möglich

Starten Sie den eDirectory-Server nach der Installation und Konfiguration von NMAS neu.

Starten Sie den eDirectory-Server neu, nachdem Sie eine Methode nach ihrer Deinstallation neu installiert haben.

17.2 Mit dem ICE-Dienstprogramm hinzugefügter Benutzer kann sich nicht mit einfachem Passwort anmelden

Verwenden Sie beim Hinzufügen von Benutzern mit dem NetIQ Import Conversion Export-Programm die Option `-l`.

18 Fehlerbehebung unter Windows

18.1 eDirectory-Server für Windows startet nicht

Wenn der eDirectory-Server beim Booten des Windows-Servers nicht startet, wird eine Meldung angezeigt, dass beim Starten des Services ein Fehler aufgetreten ist.

Wenn keine weiteren eDirectory-Datenbankreproduktionen vorhanden sind, können sich die Benutzer nicht anmelden.

Wenn andere Reproduktionen vorhanden sind, kann der Anmeldevorgang länger dauern, und es können Kommunikations- und Synchronisierungsfehler auf den Servern auftreten, auf denen sich diese Reproduktionen befinden.

- Möglicherweise wurden die eDirectory-Server-Einträge in der Windows-Registrierung bearbeitet, oder aber die Windows-Registrierung ist beschädigt.
- eDirectory-Datenbankdateien wurden möglicherweise beschädigt oder gelöscht.
- Wenn der eDirectory-Server nicht gestartet werden kann, weil ein anderer Service nicht gestartet wurde, finden Sie weitere Informationen unter *Start* > *Programme* > *Verwaltungstools* > *Ereignisanzeige*.

  Bevor Sie den eDirectory-Server starten, müssen Sie das Problem mit dem verbundenen Service beheben.
- Die Registrierung oder die ausführbaren Dateien von eDirectory sind beschädigt oder verlorengegangen. Führen Sie das SAMMIG-Dienstprogramm im Systemverzeichnis aus. Wählen Sie *NDS für NT deinstallieren* aus und schließen Sie neue eDirectory-Informationen in der NT-Domäne ein. Setzen Sie den Deinstallationsprozess bis zum Abschluss fort. Starten Sie anschließend `sammig.exe` neu und fahren Sie mit der Installation von eDirectory fort.
- Datenbankdateien wurden beschädigt oder gelöscht. Wenn der eDirectory-Server auf dem NT-Server hochgefahren wird, aber der Service die eDirectory-Datenbankdateien nicht öffnen kann, finden Sie weitere Informationen unter Abschnitt 18.2, „Der Windows-Server kann die eDirectory-Datenbankdateien nicht öffnen“, auf Seite 108.
- Der eDirectory-Server ist nicht mit einem Hub oder Schalter oder direkt mit einer Arbeitsstation verbunden (mit einer Kabelbrücke). Verbinden Sie den Server mit einem Hub oder Schalter.

18.2 Der Windows-Server kann die eDirectory-Datenbankdateien nicht öffnen

Wenn der eDirectory-Server die Datenbankdateien nicht öffnen kann, wird auf dem Windows-Server eine Meldung angezeigt.

Wenn keine weiteren Datenbankreproduktionen vorhanden sind, können sich die Benutzer nicht anmelden.

Wenn andere Reproduktionen vorhanden sind, kann der Anmeldevorgang länger dauern, und es können Kommunikations- und Synchronisierungsfehler auf den Servern auftreten, auf denen sich diese Reproduktionen befinden.

- Die Datenbankdateien wurden möglicherweise aufgrund von Festplattenfehlern auf dem Windows NT/2000-Server beschädigt.
- Möglicherweise hat jemand eine oder mehrere Datenbankdateien gelöscht.

Wenn andere Reproduktionen der eDirectory-Datenbank vorhanden sind, führen Sie die folgenden Schritte aus:

1. Starten Sie NetIQ iManager von der Verwaltungs-Arbeitsstation.
2. Entfernen Sie die beschädigte Reproduktion aus dem Reproduktionsring.

   Weitere Informationen finden Sie unter „Löschen einer Reproduktion“ im *NetIQ eDirectory 8.8 SP8-Administrationshandbuch*.
3. Führen Sie das Dienstprogramm `sammig.exe` im Systemverzeichnis auf dem NT-Server (`c:\winnt\system32`) oder über das *Start*menü aus.
4. Wählen Sie die Option zum Erstellen einer neuen Reproduktion auf dem eDirectory-Server aus.

Wenn sich auf diesem eDirectory-Server die einzige Reproduktion der Partition befindet, müssen Sie die folgenden Schritte ausführen:

1. Führen Sie das Dienstprogramm `sammig.exe` im Systemverzeichnis auf dem NT-Server (`c:\winnt\system32`) oder über das *Start*menü aus.
2. Wählen Sie unter Windows *NDS deinstallieren* aus und stellen Sie den vorherigen Windows-Domänenstatus wieder her.
3. Setzen Sie den Deinstallationsprozess bis zum Abschluss fort.
4. Starten Sie das Migrationswerkzeug neu und fahren Sie mit der Installation von eDirectory unter Windows fort.
5. Verschieben Sie die `Benutzer`objekte aus der Windows NT/2000-Domäne in den eDirectory-Baum.

18.3 SLP_NETWORK_ERROR(-23) tritt auf Windows-Maschinen auf

Die Abfrage des Service Location Protocol (SLP) gibt „-23 SLP_NETWORK_ERROR“ auf einem virtuellen Computer mit DHCP-Adresse oder auf einem physischen oder virtuellen Computer, auf dem SLP nicht übertragen wird, zurück.

Der SLP-Fehler kann vermieden werden, indem der Verzeichnisagent im Netzwerk auf eine der folgenden Weisen konfiguriert wird:

1 Kopieren Sie die Datei `C:\Windows\System32\Novell\eDir\OpenSLP\slp.conf` in das Verzeichnis `c:\Windows\`.

2 Öffnen Sie die Datei `slp.conf` mit einem Texteditor und ändern Sie die folgende Zeile:

```
;net.slp.DAAddresses = myDay1,myDa2,myDa3
```

in

```
net.slp.DAAddresses = <Give your DA Address>
```

3 Speichern Sie die Änderungen und schließen Sie die Datei.

ODER

1 Kopieren Sie die Datei `C:\Windows\System32\Novell\eDir\OpenSLP\slp.conf` in das Verzeichnis `c:\Windows\`.

2 Öffnen Sie die Datei `slp.conf` mit einem Texteditor und ändern Sie die folgende Zeile:

```
 ;net.slp.isDA = true
```

in

```
net.slp.isDA = true
```

3 Speichern Sie die Änderungen und schließen Sie die Datei.

18.4 Bei der eDirectory-Installation wird auf der Seite „Durchsuchen“ ein falscher Installationspfad angezeigt

Ändern Sie den Pfad manuell in den gewünschten Standort.

18.5 Beim Hinzufügen eines Servers tritt ein Fehler auf, wenn SLP unter Windows nicht ordnungsgemäß funktioniert ist

Beim Installieren von eDirectory tritt beim Hinzufügen eines Servers zum Baum (beim Durchsuchen des aktuellen Baums) ein Fehler auf, wenn SLPD bereits installiert ist und ausgeführt wird. In Windows wird die Meldung *launch.exe died* („launch.exe ist abgestürzt“) angezeigt.

Um eDirectory erfolgreich zu installieren, führen Sie ohne Neustart des Systems die folgenden Schritte aus:

1 Stoppen Sie den Service Location Protocol-Service.

2 Löschen Sie die Datei `C:\Windows\slp.conf`.

3. Löschen Sie den Ordner `C:\Windows\System32\Novell\eDir\OpenSLP`.
4. Löschen Sie die Registrierungsschlüssel für den SLPD-Service aus `Registry HKLM\SYSTEM\CurrentControlSet\Services\slpd`.
5. Führen Sie das Setupprogramm mit der Administratorrolle neu aus.

19 Zugriff auf HTTPSTK bei nicht geladenem DS

Sie können einen vorkonfigurierten Administratorbenutzer einrichten, der den Zugriff auf den HTTP-Protokollstapel (HTTPSTK) bei nicht geladenem DS zulässt. Der vorkonfigurierte Administratorbenutzer (sadmin) verfügt über die gleichen Rechte wie das eDirectory-Administratorbenutzerobjekt. Wenn der Server sich in einem Zustand befindet, in dem eDirectory nicht richtig funktioniert, können Sie sich mit diesem Benutzer am Server anmelden und alle Diagnose- und Fehlerbehebungsaufgaben ausführen, für die eDirectory nicht erforderlich ist.

- Abschnitt 19.1, „Festlegen des sadmin-Passworts unter Windows“, auf Seite 111
- Abschnitt 19.2, „Festlegen des sadmin-Passworts unter Linux“, auf Seite 111

19.1 Festlegen des sadmin-Passworts unter Windows

Sie können das sadmin-Passwort auf der DHost-Remoteverwaltungsseite festlegen (Zugriff über die URL `/dhost` oder über die Root-Seite). `dhost.exe` muss auf dem eDirectory-Server ausgeführt werden, damit Sie das sadmin-Passwort festlegen oder ändern können.

1. Öffnen Sie einen Webbrowser.
2. Geben Sie Folgendes in das Adressenfeld (URL) ein:

   `http://`*`server.name`*`:`*`port`*`/dhost`

   Beispiel:

   `http://MyServer:80/dhost`

   Sie können auch über die Server-IP-Adresse auf die DHost iConsole zugreifen. Beispiel:

   `http://137.65.135.150:80/dhost`
3. Geben Sie einen Benutzernamen, einen Kontext und ein Passwort ein.
4. Klicken Sie auf *HTTP-Server* und geben Sie ein sadmin-Passwort fest.
5. Überprüfen Sie das soeben eingegebene Passwort und klicken Sie auf *Senden*.

19.2 Festlegen des sadmin-Passworts unter Linux

Sie können das Passwort entweder über die DHost-Remoteverwaltungsseite oder über das ndsconfig-Dienstprogramm festlegen.

DHost-Remoteverwaltungsseite

Sie können das sadmin-Passwort auf der DHost-Remoteverwaltungsseite festlegen (Zugriff über die URL `/dhost` oder über die Root-Seite). NetIQ eDirectory-Server muss auf dem eDirectory-Server ausgeführt werden, damit Sie das sadmin-Passwort festlegen oder ändern können.

1 Öffnen Sie einen Webbrowser.

2 Geben Sie Folgendes in das Adressenfeld (URL) ein:

   http://*server.name*:*port*/dhost

   Beispiel:

   ```
   http://MyServer:80/dhost
   ```

   Sie können auch über die Server-IP-Adresse auf die DHost iConsole zugreifen. Beispiel:

   ```
   http://137.65.135.150:80/dhost
   ```

3 Geben Sie einen Benutzernamen, einen Kontext und ein Passwort ein.

4 Klicken Sie auf *HTTP-Server* und geben Sie ein sadmin-Passwort fest.

5 Überprüfen Sie das soeben eingegebene Passwort und klicken Sie auf *Senden*.

ndsconfig

Legen Sie das sadmin-Passwort mit dem ndsconfig-Dienstprogramm fest. „ndsd“ muss auf dem eDirectory-Server ausgeführt werden, damit Sie das sadmin-Passwort festlegen oder ändern können.

Geben Sie an der Serverkonsole Folgendes ein

```
ndsconfig set http.server.sadmin-pwd=Passwort
```

Password muss durch das neue sadmin-Passwort ersetzt werden.

Weitere Informationen zur Verwendung des ndsconfig-Dienstprogramms finden Sie unter „Parameter des ndsconfig-Dienstprogramms“ im *NetIQ eDirectory 8.8 SP8-Installationshandbuch*.

20 Verschlüsseln von Daten in eDirectory

In NetIQ eDirectory 8.8 und höheren Versionen können Sie bestimmte vertrauliche Daten zum Speichern auf dem Datenträger und für den Zugriff durch den Client verschlüsseln. Dieses Kapitel enthält Informationen zur Behebung von Fehlern, die beim Verwenden verschlüsselter Attribute und Reproduktionsfunktionen in eDirectory 8.8 und höheren Versionen auftreten können. Weitere Informationen zu verschlüsselten Attributen und zur Reproduktion finden Sie im *NetIQ eDirectory 8.8 SP8.Administrationshandbuch* (http://www.netiq.com/documentation/edir88/edir88/data/a2iii88.html).

Informationen zu Fehlermeldungen in eDirectory finden Sie auf der Website zu NetIQ-Fehlermeldungen (http://www.novell.com/documentation/nwec/).

20.1 Fehlermeldungen

Dieser Abschnitt enthält Informationen zu den folgenden Fehlermeldungen:

20.1.1 -6090 0xFFFFE836 ERR_ER_DISABLED

Vom eDirectory-Reproduktionssynchronisierungsprozess wurde versucht, eine verschlüsselte Reproduktion mit dem Zielserver einzuleiten. Auf dem eDirectory-Zielserver ist der Prozess für die verschlüsselte Reproduktionssynchronisierung jedoch deaktiviert.

Mögliche Ursache

Die verschlüsselte Reproduktion ist auf dem eDirectory-Zielserver deaktiviert.

Aktion

Aktivieren Sie die verschlüsselte Reproduktion auf dem eDirectory-Zielserver.

20.1.2 -6089 0xFFFFE837 ERR_REQUIRE_SECURE_ACCESS

Eine Anwendung (Clientzugriff) hat versucht, über einen Klartextkanal auf ein verschlüsseltes Attribut zuzugreifen.

Quelle

eDirectory oder NDS

Mögliche Ursache

Die verschlüsselten Attribute sind so konfiguriert, dass der Zugriff nur über einen sicheren Kanal erfolgen kann. Die Anwendung versucht, über einen Klartextkanal auf die verschlüsselten Attribute zuzugreifen.

Aktion

Die Anwendung muss über einen sicheren Kanal wie einen sicheren LDAP-Kanal oder einen sicheren HTTP-Kanal auf die verschlüsselten Attribute zugreifen.

Mögliche Ursache

Wenn dieser Fehler während einer Reproduktion auftritt, sind auf einem oder mehreren Servern im Reproduktionsring bestimmte Attribute zur Verschlüsselung gekennzeichnet und so konfiguriert, dass nur über einen sicheren Kanal auf sie zugegriffen werden kann.

Aktion

Ändern Sie die Konfiguration der Richtlinie für die verschlüsselten Attribute so, dass über unsichere Kanäle auf verschlüsselte Attribute werden kann. Weitere Informationen finden Sie im *NetIQ eDirectory 8.8 SP8-Administrationshandbuch* (http://www.netiq.com/documentation/edir88/edir88/data/a2iii88.html).

Mögliche Ursache

Wenn dieser Fehler auftritt, wenn die verschlüsselte Reproduktion auf der Partitionsebene oder zwischen Reproduktionen einer Partition konfiguriert ist, sind im Reproduktionsring Server mit einer Version unter eDirectory 8.8 vorhanden.

Aktion

Rüsten Sie alle Server im Reproduktionsring auf eine mit eDirectory 8.8 kompatible Version auf.

20.1.3 -666 FFFFFD66 INCOMPATIBLE NDS VERSION

Hier steht Text

Mögliche Ursache

Wenn die verschlüsselte Reproduktion auf Partitionsebene aktiviert ist und Sie versuchen, eine Reproduktion dieser Partition zu einem eDirectory-Server hinzuzufügen, ist die eDirectory-Version des Servers nicht mit der Version des Ursprungsservers kompatibel.

Aktion

Rüsten Sie den Server auf eine kompatible eDirectory-Version auf.

Mögliche Ursache

Wenn in der übergeordneten Partition Server mit einer Version vor eDirectory 8.8 vorhanden sind (Ring mit gemischten Versionen) und auf der untergeordneten Partition ER aktiviert ist, sind die Vorgänge zum Zusammenführen und/oder Verknüpfen von Partitionen nicht zulässig und der Fehler „ERR_INCOMPATIBLE_DS_VERSION“ wird zurückgegeben.

Dies liegt daran, dass die untergeordnete Partition vertrauliche Daten mit verschlüsselter Reproduktion auf Partitionsebene enthält und auf der übergeordneten Partition ein Server mit einer Version vor eDirectory 8.8 vorhanden ist. Wenn die verschlüsselte Reproduktion nur zwischen eDirectory 8.8-Servern aktiviert ist, werden vertrauliche Daten bei der Reproduktion zu Servern mit einer Version vor eDirectory 8.8 beim Zusammenführen ausgesetzt.

Aktion

1. Rüsten Sie den Server auf eine kompatible eDirectory-Version auf.

   ODER
2. Deaktivieren Sie die verschlüsselte Reproduktion in der übergeordneten oder untergeordneten Partition.

   HINWEIS: Nach der Deaktivierung der verschlüsselten Reproduktion wird die Reproduktion im Klartextformat ausgeführt.

20.2 Problem mit doppelten Verschlüsselungsalgorithmen

Wenn Sie ein Attribut zur Verschlüsselung mit LDIF hinzufügen, verknüpfen Sie keine doppelten Algorithmen mit einem Attribut.

Wenn beispielsweise *title* als verschlüsseltes Attribut mit den Verschlüsselungsalgorithmen AES und DES gekennzeichnet wird, ist unklar, welcher Algorithmus im Endeffekt berücksichtigt wird. Bei jedem Ausführen von Limber wechselt das title-Attribut zwischen AES und DES. Daher erscheint es so, als ob Konfigurationsänderungen vorgenommen wurden.

Um ein solches Szenario zu vermeiden, empfiehlt es sich, keine doppelten Algorithmen zum gleichen Attribut zuzuweisen.

Dies ist nicht der Fall, wenn Sie Sie ein Attribut mit iManager zur Verschlüsselung kennzeichnen.

20.3 Verschlüsselung von Stream-Attributen

Stream-Attribute können als Klartextdaten vorliegen. Dies liegt daran, dass eDirectory 8.8 Stream-Attribute nicht verschlüsselt.

20.4 Konfigurieren der verschlüsselten Reproduktion über iManager

Die verschlüsselte Reproduktion kann nicht über iManager konfiguriert werden, wenn einer der Server im Reproduktionsring abgeschaltet ist.

20.5 Anzeigen oder Ändern verschlüsselter Attribute über iManager

Wenn ein Attribut eines Objekts verschlüsselt ist, können Sie das Objekt nicht mit iManager 2.5 anzeigen oder ändern.

Um dieses Problem zu umgehen, können Sie die verschlüsselten Attribute mit einem der folgenden Verfahren über einen sicheren Kanal anzeigen oder ändern:

- LDAP: Die LDAP-Anfrage muss über einen sicheren Kanal gesendet werden, das heißt, das Herkunftsverbürgungszertifikat des Servers muss verwendet werden.
- ICE: Zum Ändern des Objekts können LDIF-Skripts verwendet werden. ICE muss dann einen sicheren Kanal verwenden.
- Verwenden Sie iManager 2.5 FP2, iManager 2.6 oder eine höhere Version.

HINWEIS: Zum Anzeigen oder Bearbeiten verschlüsselter Attribute wird iManager 2.6 oder höher empfohlen.

Alternativ können Sie die Option, die einen sicheren Kanal anfordert, für das Anzeigen und Ändern verschlüsselter Attribute abschalten, indem Sie das Attribut `requireSecure` in der EA-Richtlinie deaktivieren. Der Zugriff auf das Objekt und die verschlüsselten Attribute ist dann für jeden Client über einen Klartextkanal möglich. Danach ist iManager in der Lage, auf das Objekt zuzugreifen.

20.6 Zusammenführen von Bäumen mit verschlüsselter Reproduktion nicht möglich

Wenn die verschlüsselte Reproduktion aktiviert ist, ist das Zusammenführen von Bäumen nicht möglich. Deaktivieren Sie die sichere Reproduktion auf jedem Baum, bevor Sie eine Zusammenführung vornehmen.

20.7 Limber zeigt Fehler -603 an

Limber zeigt den Fehler -603 an, wenn der Server nur eine untergeordnete Referenzreproduktion der Partition mit dem verschlüsselten Attribut der Richtlinie hat.

Dieses Problem lässt sich mit folgenden Verfahren umgehen:

- Erteilen Sie Lesezugriff auf das NCP-Serverobjekt. Hierzu können Sie in iManager wie folgt vorgehen: Fügen Sie einen Trustee am Stamm des Baums hinzu und erteilen Sie Lesezugriff auf das NCP-Serverobjekt. Geben Sie in den Attributen `attrEncryptionDefinition` und `attrEncryptionRequiresSecure` an.
- Erteilen Sie öffentlichen Lesezugriff auf die folgenden Attribute über LDAP oder ndssch:
    - `attrEncryptionDefinition`
    - `attrEncryptionRequiresSecure`

21 Die eDirectory Management Toolbox

Mit der NetIQ eDirectory Management Toolbox (eMBox) können Sie remote und auf dem Server auf alle eDirectory-Backend-Dienstprogramme zugreifen.

eMBox bietet in Verbindung mit NetIQ iManager webbasierten Zugriff auf eDirectory-Dienstprogramme wie DSRepair, DSMerge, Backup and Restore und Service Manager.

WICHTIG: Die rollenbasierten Services müssen über iManager für den zu verwaltenden Baum konfiguriert sein, damit eMBox-Aufgaben ausgeführt werden können.

Alle Funktionen können entweder auf dem lokalen Server oder entfernt über einen Befehlszeilen-Client aufgerufen werden. Sie können mit dem eMBox-Client Aufgaben für mehrere Server von einem Server oder einer Arbeitsstation aus durchführen. Zum Ausführen der eDirectory Management Tools (eMTools), wie Backup, DSRepair, DSMerge, Schema Operations und eDirectory Service Manager, muss eMBox geladen sein und auf dem eDirectory-Server ausgeführt werden.

- Abschnitt 21.1, „eMTool-Services können nicht gestoppt werden“, auf Seite 117
- Abschnitt 21.2, „Bei der Wiederherstellung wird der Fehler -6020 zurückgegeben“, auf Seite 117
- Abschnitt 21.3, „Probleme mit dem eDirectory Service-Manager“, auf Seite 118

21.1 eMTool-Services können nicht gestoppt werden

Beim Ausführen des Befehls `serviceStop -n`*{service}* (*{service}* ist dabei einer der Services `libsasl.so`, `libncpengine.so`, `libhttpstk.so` oder `libdsloader.so`) tritt folgender Fehler auf:

```
Service {service} could not be stopped, Error : -660
```

Dies ist kein Fehler. Sie können diese Prozesse (insbesondere `libsasl.so`, `libncpengine.so`, `libhttpstk.so` und `libdsloader.so`) nicht stoppen, weil andere Module von ihnen abhängen.

21.2 Bei der Wiederherstellung wird der Fehler -6020 zurückgegeben

Wenn Rollforward-Protokolle an einem Standardspeicherort vorhanden sind, tritt beim Ausführen eines Wiederherstellungsvorgangs mit DSBK oder dem eMBox-Client der Fehler -6020 auf. Verwenden Sie den Schalter `-s` im `restore`-Befehl, um diesen Fehler zu vermeiden.

21.3 Probleme mit dem eDirectory Service-Manager

Wenn Sie den eDirectory Service-Manager in iManager zum Anhalten von eDirectory verwenden, ist der Neustart mit dem Service-Manager nicht möglich. Verwenden Sie das Dienstprogramm eDirectory Services (`C:\novell\NDS\NDSCons.exe`) auf dem eDirectory-Server, um eDirectory neu zu starten.

21.3.1 Löschen eines verschobenen Objekts

In einer aus mehreren Servern bestehenden Baumstruktur lässt sich ein verschobenes Objekt unter Umständen nicht löschen (error -637).

21.3.2 Problem beim Verschieben einer dynamischen Gruppe

Beim Verschieben eines dynamischen Gruppenobjekts zu einem anderen Container wird die Funktionalität der dynamischen Gruppe unterbrochen, wenn das Attribut `Objektklasse dynamicgroup` beinhaltet. Nach dem Verschieben funktionieren Abfragen und Suchen nach dynamischen Mitgliedern nicht mehr.

21.3.3 Problem beim Reparieren von Netzwerkadressen durch eMBox

Beim Reparieren der Netzwerkadressen durch eMBox werden folgende Fehlermeldungen ausgegeben, weil eMBox nicht mit den aktuellen Fixes für die Reparatur aktualisiert ist:

```
FEHLER: Keine Netzwerkadresse für diesen Server gefunden - Fehler: 11004
```

```
FEHLER: Verbindung nicht möglich. Fehler: 11004
```

21.3.4 Anzeigen der französischen man-Seiten

Um französische man-Seiten unter Red Hat Linux anzuzeigen, exportieren Sie Folgendes:

```
export MANPATH=/opt/novell/man/frutf8:/opt/novell/eDirectory/man/frutf8
```

21.3.5 Löschen eines verschobenen Objekts

In einer aus mehreren Servern bestehenden Baumstruktur lässt sich ein verschobenes Objekt unter Umständen nicht löschen (error -637).

21.3.6 eDirectory generiert kein Abmeldeereignis aufgrund der eDirectory-Client-Beschränkung

eDirectory erstellt kein Abmeldeereignis, wenn Sie sich von iManager abmelden. Dies liegt an einer technischen Beschränkung im Client-Bereich von eDirectory.

Revisionsanwendungen können Abmeldeereignisse mithilfe von NWDS APIs empfangen. Anwendungen, die LDAP verwenden, können die Abmeldung mit Unbind-Ereignissen überwachen.

21.3.7 Probleme durch TERM beim Ausführen von DSTrace

TIME und TAGS werden als aktiviert dargestellt (unterstrichen), jedoch nicht standardmäßig. Wird TERM von einem Linux-Terminal auf VT100 oder xterm gesetzt, werden diese Tags als aktiviert dargestellt (unterstrichen). Das Problem tritt nicht bei anderen Terms auf, z. B. dtterm.

21.3.8 eMBox verarbeitet keine Doppelbytezeichen

eMBox verarbeitet keine Doppelbytezeichen beim Festlegen eines Rollforwardverzeichnisses durch den eMBox-Client und iManager. Dies kann jedoch über DSBK erfolgen.

22 SASL-GSSAPI

Dieser Abschnitt enthält Informationen zu den Fehlermeldungen, die vom Authentifizierungsmechanismus SASL-GSSAPI protokolliert werden.

22.1 Probleme im Zusammenhang mit SASL-GSSAPI

22.1.1 Problem mit mehreren Benutzerobjekten

Bei der LDAP-Bindung mit SASL GSSAPI tritt ein Fehler auf, wenn das gleiche Kerberos-Prinzipal mit mehreren eDirectory-Benutzerobjekten verknüpft ist.

22.1.2 Berechtigungs-ID

RFC2222 legt die Unterstützung einer durch den Benutzer und den Client gesendeten Berechtigungs-ID fest. Dies wird von der SASL GSSAPI-Methode nicht unterstützt.

22.2 Protokolldatei

In Linux-Installationen werden Fehlermeldungen in der Datei `ndsd.log` protokolliert.

22.3 Fehlermeldungen

SASL-GSSAPI: Reading Object *user_FDN* FAILED *eDirectory-Fehlercode* (Fehler beim Lesen des user_FDN-Objekts)

Ursache: Dieser Fehler wird in eDirectory generiert. Das Objekt `user_FDN` ist nicht vorhanden.

SASL-GSSAPI: Reading principal names for *user_FDN* failed *eDirectory-Fehlercode* (Fehler beim Lesen der Prinzipalnamen für user_FDN)

Ursache: Dieser Fehler wird in eDirectory generiert. Der Kerberos-Prinzipalname ist nicht mit dem Benutzerobjekt (`userdn`) verknüpft.

SASL-GSSAPI: Reading Object *Realm_FDN* FAILED *eDirectory-Fehlercode* (Fehler beim Lesen des Realm_FDN-Objekts)

Ursache: Dieser Fehler wird in eDirectory generiert. Das Objekt `realm` ist nicht vorhanden.

SASL-GSSAPI: Not enough memory (Nicht genügend Arbeitsspeicher)

Ursache: Zum Ausführen der bestimmten Operation ist nicht ausreichend Arbeitsspeicher verfügbar.

SASL-GSSAPI: Invalid Input Token (Ungültiges Eingabe-Token)

Ursache: Das Token vom Client ist beschädigt oder ungültig.

SASL-GSSAPI: NMAS error *NMAS-Fehlercode* (NMAS-Fehler)

Ursache: Dieser Fehler wird in NMAS generiert und ist ein interner Fehler.

SASL-GSS: Invalid LDAP service principal name *LDAP_service_principal_name* (Ungültiger LDAP-Service-Prinzipalname)

Ursache: Der LDAP-Service-Prinzipalname ist ungültig.

SASL-GSS: Reading LDAP service principal key from eDirectory failed (Fehler beim Lesen des LDAP-Service-Prinzipalschlüssels aus eDirectory)

Ursache: Das LDAP-Service-Prinzipalobjekt ist nicht erstellt.

Ursache: Der Masterschlüssel des Bereichobjekts wurde geändert.

Ursache: Das LDAP-Service-Prinzipalobjekt wurde im Teilbaum des Bereichs, zu dem es gehört, nicht gefunden.

SASL-GSS: Creating GSS context failed (Fehler beim Erstellen des GSS-Kontexts)

Ursache: Die Uhrzeit zwischen dem Client, den KDC- und den eDirectory-Servern ist nicht synchronisiert.

Ursache: Der Schlüssel des LDAP-Service-Prinzipals wurde in der Kerberos-Datenbank geändert, jedoch in eDirectory nicht aktualisiert.

Ursache: Der Verschlüsselungstyp wird nicht unterstützt.

SASL GSSAPI: Invalid user FDN = *user_FDN* (Ungültiger Benutzer-FDN)

Ursache: Der vom Client angegebene Benutzer-FDN ist nicht gültig.

SASL GSSAPI: No user DN is associated with principal *client_principal_name* (Mit dem Client-Prinzipalnamen ist kein Benutzer-DN verknüpft)

Ursache: Ein `Benutzer`objekt unter dem Teilbaum ist nicht mit dem Kerberos-Prinzipalnamen verknüpft.

SASL GSSAPI: More than one user DN is associated with principal *client_principal_name* (Mit dem Client-Prinzipalnamen sind mehr als ein Benutzer-DN verknüpft)

Ursache: Mehr als ein `Benutzer`objekt unter dem Teilbaum ist mit dem gleichen Prinzipal verknüpft.

ldap_simple_bind_s: Invalid credentials major = 1, minor =0 (Ungültiger Berechtigungsnachweis, oberer=1, unterer=0)

Ursache: Dies kann durch nicht übereinstimmende Versionen des LDAP-Service-Prinzipals auf dem KDC-Server und des LDAP-Service-Prinzipals auf dem eDirectory-Server verursacht sein. Dies liegt daran, dass die Versionsnummer jedes Mal erhöht wird, wenn der LDAP-Service-Prinzipalschlüssel in die Schlüsseltabellendatei extrahiert wird.

Aktion:

Führen Sie die folgende Prozedur aus:

1. Aktualisieren Sie den Schlüssel auf dem eDirectory-Server so, dass die Versionsnummern synchronisiert sind.
2. Vernichten Sie die Tickets auf dem Client.
3. Rufen Sie erneut den TGT für den Prinzipal ab.
4. Führen Sie die LDAP-Bindungsoperation `sasl` aus.

23 Sonstige

23.1 Sichern eines Containers

Wenn ein Container mit vielen Objekten (beispielsweise einer Million) mit „ndsbackup“ gesichert wird, kann es einige Zeit dauern, bis die Liste der Objekte im Container abgerufen wird und die einzelnen Sicherungen gestartet werden.

23.2 Wiederholte eDirectory-Anmeldungen

Wiederholte eDirectory-Anmeldungen können den verfügbaren Arbeitsspeicher auslasten. Deaktivieren Sie mit iMonitor das Anmeldeaktualisierungsattribut, um dieses Problem zu umgehen.

23.3 Aktivieren der Ereignissystemstatistiken

Für jedes in eDirectory ausgegebene und verbrauchte Ereignis werden zeitbezogene Statistiken gepflegt. Diese Informationen sind hilfreich zur Behebung von Problemen mit Ereignisverbrauchern. Die Statistiken sind für das normale Funktionieren des Verzeichnisses nicht erforderlich und daher aus Leistungsgründen deaktiviert. Die Ereignisstatistiken können während der Laufzeit über die erweiterten Konfigurationsparameter in iMonitor aktiviert werden.

Um die Ereignisstatistiken anzuzeigen, setzen Sie den Parameter `ENABLE_EVENT_STATISTICS` und starten Sie den Server neu. Es handelt sich um einen dauerhaften Konfigurationsparameter.

23.4 Statusüberwachung von Arbeitsspeicherbeschädigungsproblemem unter Linux

Auf Linux-Plattformen verwendet eDirectory Google-malloc (`libtcmalloc`) als standardmäßigen Arbeitsspeicherzuordner.

Um Probleme mit der Arbeitsspeicherbeschädigung zu überwachen, setzen Sie im ndsd-Startskript die Umgebungsvariable `MALLOC_CHECK_`. Das Startskript sucht nach dieser Variable. Wenn die Variable gesetzt ist, wird der standardmäßige Arbeitsspeicherzuordner des Systems verwendet; andernfalls wird `libtcmalloc` geladen.

MALLOC_CHECK-Einstellungen in „ndsd“

* Wenn `MALLOC_CHECK_` auf 0 festgelegt ist, werden erkannte Heapbeschädigungen still ignoriert.
* Wenn `MALLOC_CHECK_` auf 2 gesetzt wird, wird sofort der Abbruch aufgerufen.

  Dies hilft dabei, die eigentliche Ursache der Speicherbeschädigung in einem frühen Stadium zu erkennen, nicht erst später, wenn dies schwieriger ist.

23.5 TCP-Verbindung wird nach nicht ordnungsgemäßer Abmeldung nicht beendet

In einigen Fällen erkennt der OES Linux-Server nicht einen Client-Host, der aufgrund des Ausfalls einer Arbeitsstation oder eines Stromausfalls unerwartet heruntergefahren wurde. Die Verbindung bleibt jedoch für die Dauer der standardmäßigen Zeitüberschreitung (etwa 12 bis 15 Minuten) bestehen, bevor sie gelöscht wird. Wenn Sie die Anzahl der gleichzeitigen Verbindungen auf 1 gesetzt haben, sollten Sie die Verbindung entweder manuell beenden oder die geschätzte Zeitüberschreitung abwarten, bevor Sie sich erneut anmelden. Diese Situation tritt ein, wenn der Überwachungsprozess die Verbindung nicht sauber schließt. Wenn die Anzahl der gleichzeitigen Verbindungen auf 1 festgelegt ist und die Verbindung vom Überwachungsprozess nicht gelöscht wird, können sich die Benutzer nicht anmelden. Der Linux-Kernel bietet drei Parameter, mit denen festgelegt werden kann, wie `keepalive`-Muster von der Serverseite aus arbeiten. Stellen Sie mit diesen Parametern eine Behelfslösung auf TCP-Ebene bereit.

Die Parameter stehen im Verzeichnis `/proc/sys/net/ipv4/` zur Verfügung.

- `tcp_keepalive_time`: Bestimmt die Frequenz, mit der TCP-`keepalive`-Pakete gesendet werden, um eine derzeit nicht verwendete Verbindung aktiv zu erhalten. Dieser Wert wird nur verwendet, wenn `keepalive` aktiviert ist.

  Für `tcp_keepalive_time` wird ein ganzzahliger Wert in Sekunden angegeben. Der Standardwert ist 7200 Sekunden bzw. 2 Stunden. Dies ist für die meisten Hosts gut geeignet und beansprucht die Netzwerkressourcen nicht zu stark. Wenn Sie einen zu niedrigen Wert festlegen, werden die Netzwerkressourcen mit unnötigem Datenverkehr belastet.
- `tcp_keepalive_probes`: Bestimmt die Frequenz, mit der TCP-`keepalive`-Muster gesendet werden, bevor eine unterbrochene Verbindung entschieden wird.

  Für `tcp_keepalive_probes` wird ein ganzzahliger Wert festgelegt. Je nach den Werten für `tcp_keepalive_time` und `tcp_keepalive_interval` empfiehlt sich ein Wert unter 50. Standardmäßig wird die Anwendung nach 9 Mustern über die unterbrochene Verbindung informiert.
- `tcp_keepalive_intvl`: Bestimmt die Dauer der Antwort für jedes `keepalive`-Muster. Dieser Wert ist wichtig für die Berechnung der Dauer, nach der die Verbindung eine `keepalive`-Unterbrechung erfährt.

  Für `tcp_keepalive_intvl` wird ein ganzzahliger Wert, standardmäßig 75 Sekunden, festgelegt. 9 Muster zu jeweils 75 Sekunden dauern also etwa 11 Minuten. Anhand der standardmäßigen Werte für die Variablen `tcp_keepalive_probes` und `tcp_keepalive_intvl` kann geschätzt werden, nach welcher Zeitdauer bei einer Verbindung eine `keepalive`-Zeitüberschreitung auftritt.

Bearbeiten Sie diese drei Parameter so, dass kein übermäßiger zusätzlicher Netzwerkverkehr generiert, das Problem jedoch behoben wird. Eine Änderung könnte wie folgt aussehen (3-minütige Erkennungsdauer):

- `tcp_keepalive_time set -120`
- `tcp_keepalive_probes - 3`
- `tcp_keepalive_intvl - 20`

HINWEIS: Ändern Sie die Parametereinstellungen mit Vorsicht und vermeiden Sie das Einstellen bereits gültiger Verbindungen.

Die Einstellungen sind sofort nach dem Ändern der Dateien wirksam. Es ist nicht erforderlich, Services neu zu starten. Die Einstellungen sind jedoch nur für die aktuelle Sitzung gültig. Nach dem Neubooten des Servers werden die Einstellungen auf die standardmäßigen Einstellungen zurückgesetzt.

Gehen Sie folgendermaßen vor, um die Einstellung dauerhaft (auch nach einem erneuten Booten) anzuwenden:

Fügen Sie die folgenden Einträge zu `/etc/sysctl.conf` hinzu.

- net.ipv4.tcp_keepalive_time=120
- net.ipv4.tcp_keepalive_probes=3
- net.ipv4.tcp_keepalive_intvl=20

Diese Einstellungen werden nur empfohlen, wenn alle Clients und Server über LAN verbunden sind.

23.6 NDS-Fehler „Systemfehler“ (-632) tritt auf, wenn „ldapsearch“ für die Benutzerobjekte ausgeführt wird

Importieren Sie die Benutzerobjekte mit einfachem Passwort und aktivieren Sie dann ein universelles Passwort für den Container, in den die Benutzerobjekte importiert werden. Stoppen Sie den DS-Server und legen Sie für die Umgebung `NDSD_TRY_NMASLOGIN_FIRST=true` fest. Starten Sie dann den DS-Server. Wenn Sie ein „ldapsearch“ für die Benutzerobjekte ausführen, die mit einfachem Passwort importiert wurden, tritt folgender Fehler auf:

```
ldap_bind: Unknown error,  additional info: NDS error: system failure (-632)
```

Um das Problem zu beheben, legen Sie als standardmäßige Anmeldesequenz für den Container, in den die Benutzerobjekte importiert werden, ein einfaches Passwort fest, bevor „ldapsearch“ auf den Benutzerobjekten ausgeführt wird.

Wenn LDAP eine Anmeldung von NMAS als Benutzer anfordert, verwendet NMAS die standardmäßige Anmeldesequenz. Wenn Sie für diese Benutzer keine standardmäßige Anmeldesequenz festlegen, wird die NDS-Sequenz verwendet. Wenn den Benutzern beim Importieren kein NDS-Passwort gegeben wird, funktioniert die NDS-Sequenz nicht. Wenn Sie universelle Passwörter aktivieren, wird das einfache Passwort mit dem NDS-Passwort und dem universellen Passwort synchronisiert, wenn sich der Benutzer mit dem einfachen Passwort anmeldet.

23.7 Deaktivieren von SecretStore

Ein eDirectory-Administrator kann SecretStore mit den folgenden Prozessen deaktivieren:

23.7.1 Unter Linux

1. Wechseln Sie zum Verzeichnis `nds-modules` und benennen Sie folgende SecretStore-Module um bzw. verschieben Sie sie:

   ```
   libsss.so
   libssncp.so
   libssldp.so
   ```

2. Starten Sie den Server neu.

Alternativ können Sie die Zeile in der Datei `/etc/opt/novell/eDirectory/conf/ndsmodules.conf` auskommentieren, in der „ssncp“ geladen wird.

23.7.2 Unter Windows

1 Wechseln Sie zum Verzeichnis `novell\nds` und benennen Sie folgende SecretStore-Module um bzw. verschieben Sie sie:

   `lsss.dll`

   `sss.dlm`

   `ssncp.dlm`

   `ssldp.dlm`

2 Starten Sie den Server neu.

23.8 Anzeigen der Manpages für SLP

Zum Anzeigen der Manpages für SLP müssen Sie die Pfade für die Manpages festlegen. Beispielsweise müssen Sie unter AIX den Manpath auf `/usr/share/man` anstatt auf `/opt/novell/man` festlegen.

23.9 Speicherort der dsbk-Konfigurationsdatei

Die Datei `dsbk.conf` ist im Verzeichnis `/etc` gespeichert, nicht an dem relativ zur jeweiligen Instanz von eDirectory befindlichen Speicherort.

23.10 Probleme mit der SLP-Interoperabilität unter OES Linux

OpenSLP implementiert SLPv2, doch NetIQ SLP (NDSslp) auf Linux- und Windows-Plattformen implementiert SLPv1.

SLPv1 UAs erhalten keine Antworten von SLPv2 SAs und SLPv2 UAs erhalten keine Antworten von SLPv1 SAs. Dies bedeutet, dass die Clients mit OpenSLP keine Bäume mit NDSslp "sehen" können. Ebenso können die Clients mit NDSslp keine Bäume mit OpenSLP "sehen". Damit SLPv1 und SLPv2 interagieren, müssen Sie einen DA konfigurieren, der SLPv2 ausführt. Wenn eDirectory unter Linux-Plattformen wie Red Hat Linux installiert ist, kann es ggf. NDSslp verwenden, das in eDirectory enthalten ist. Aufgrund von Interoperabilitätsproblemen mit den beiden Versionen von SLP ist ein über OpenSLP-Multicast bekannt gegebener Baum für NDSslp ggf. nicht sichtbar und umgekehrt. Zur Behebung dieses Problems müssen Sie einen DA konfigurieren, der OpenSLP ausführt.

23.11 Die Fehlerprotokolldatei von Ldif2dib kann nicht geöffnet werden, wenn sich das DIB-Verzeichnis in einem benutzerdefinierten Pfad befindet

Die Standardprotokolldatei von ldif2dib, `ldif2dib.log`, kann nicht geöffnet werden, wenn das `dib`-Verzeichnis an einen benutzerdefinierten Speicherort verschoben wird.

Zur Umgehung dieses Problems geben Sie den Speicherort der Protokolldatei explizit mit dem Schalter `-b` an.

23.12 eDirectory-Server wird auf virtuellem SLES 10 nicht automatisch hochgefahren

Wenn Sie eDirectory nach dem Hinzufügen von Paketen nicht mit YaST konfigurieren, müssen Sie folgenden Befehl an der Kommandozeile ausführen.

```
chkconfig -a ndsd
```

23.13 ndsd wird nach einem Systemabsturz nicht gestartet

In einigen Fällen werden die eDirectory-Dienste (ndsd) nach einem Systemabsturz oder einem Stromausfall nicht neu gestartet. Führen Sie die folgenden Schritte aus, um eDirectory neu zu starten:

1. Löschen Sie die Datei /var/opt/novell/eDirectory/data/ndsd.pid.
2. Geben Sie den Befehl /etc/init.d/ndsd start ein.

23.14 DSTrace nicht auf Linux-Computern ausführen, wenn alle Kennungen aktiviert sind

Wenn alle Kennungen aktiviert sind, stellen Sie sicher, dass Sie DSTrace nicht ausführen unter:

- **Einem geladenen System im Journal-Modus:** Der ndsd-Arbeitsspeicher wächst dabei tendenziell an.
- **Server im Inlinemodus:** „ndsd“ stürzt dabei ab.

23.15 LDAP ist nicht RFC-kompatibel für anonyme Suchanfragen

Wenn ein Client eine nicht autorisierte Suchaktion durchführt und anonyme Bindungen deaktiviert sind, antwortet der LDAP-Server mit dem Bindungsergebnis einer unzureichenden Autorisierung anstelle des Suchergebnisses operationsError.

23.16 Fehlerbehebung für Ports bei benutzerdefinierten eDirectory 8.8-Instanzen

Wenn sie in eDirectory 8.8 eine neue Instanz in einem benutzerdefinierten Pfad konfigurieren, während der Standardinstanzenserver ausgeschaltet ist, werden die Ports der Standardinstanz übernommen. Die Standardinstanz wird nicht geladen, da die Ports der Standardinstanz an die benutzerdefinierte Standortinstanz vergeben sind.

Führen Sie vor einem Neustart des Hosts das unter „Fehlerbehebung für Ports bei benutzerdefinierten eDirectory 8.8-Instanzen“ (http://www.novell.com/coolsolutions/feature/17933.html) beschriebene Verfahren aus.

23.17 Neustart des Hosts

Nach dem Neustart wird nur die mit den Standardinstanz-Binärdaten erstellte Standardinstanz gestartet.

Zum Starten der anderen Instanzen können Sie die Pfade festlegen und ndsmanage verwenden.

23.18 ndsd überwacht den in der Loopback-Adresse angegebenen NCP-Port nicht

Bei mehreren eDirectory-Instanzen versuchen alle Instanzen ab der zweiten Instanz, den Standardport 524 anstelle des in der Loopback-Adresse angegebenen NCP-Ports zu überwachen.

Zur Umgehung dieses Problems stellen Sie den Parameter n4u.server.tcp-port ab der zweiten Instanz auf den Port ein, den die Instanz überwachen soll. Der Parameter "n4u.server.tcp-port" befindet sich in der Datei `nds.conf`.

WICHTIG: Alle eDirectory-Instanzen müssen hochgefahren sein, bevor Sie auf eDirectory 8.8 SP8 aufrüsten.

23.19 LDAP-Transaktions-OIDs

Bei der LDAP-Transaktionsunterstützung sind die OIDs `supportedGroupingTypes` und `transactionGroupingType` identisch (`2.16.840.1.113719.1.27.103.7`).

23.20 Fehler -5871 und -5875 im LDAP-Trace

Die Fehler -5871 und -5875 im LDAP-Trace werden üblicherweise dadurch verursacht, dass der LDAP-Client zum Schließen gezwungen wird, ohne die Bindung aufzuheben. Die Fehler müssen daher nicht beachtet und können ignoriert werden. Weitere Informationen zu diesen Fehlern finden Sie auf der Website zu NetIQ-Fehlercodes (http://www.novell.com/documentation/nwec/).

23.21 NDSCons gibt den Fehler -625 aus, wenn ein Baum umbenannt wird

Wenn Sie den Baum auf dem Primärserver umbenennen und den DHost auf dem Sekundärserver herunterfahren, gibt das NDSCons-Dienstprogramm auf dem Sekundärserver die Transportfehlermeldung -625 aus, während DHost sowohl auf dem Primär- als auch auf dem Sekundärserver weiter ausgeführt wird. Der Fehler tritt auf, weil NDSCons auf dem Sekundärserver ausgeführt wurde, als der Baum auf dem Primärserver umbenannt wurde. NDSCons arbeitet ordnungsgemäß, wenn Sie es schließen und dann erneut starten.

23.22 Das Überwachen mehrerer NICs verringert die eDirectory-ldapsearch-Suchleistung

So können Sie das Problem umgehen,

Deaktivieren Sie in der Konfigurationsdatei die NICs, die die ldapsearch-Suchleistung reduzieren.

Alternativ:

Aktivieren Sie das Advanced Referral Costing (ARC) mit dem Befehl `set NDSTRACE =!ARC1` in DSTrace.

23.23 Anzahl der gleichzeitigen Benutzer auf Linux-Plattformen kann nicht beschränkt werden

In eDirectory 8.8 SP8 kann die Anzahl der gleichzeitigen Verbindungen auf Linux-Plattformen nicht eingeschränkt werden. Um das alte Verhalten wiederherzustellen (strikte portbasierte Prüfung), stellen Sie in der Datei `nds.conf` folgende Parameter ein.

```
n4u.server.mask-port-number=0
```

23.24 Fehler beim Herunterfahren von „ndsd“ aufgrund von SLP

Wenn im Netzwerk kein SLP-Verzeichnisagent (DA) konfiguriert ist, kann es länger dauern, bis Services gefunden werden, die SLP verwenden. Beim Herunterfahren von eDirectory versucht ndsd, Operationen mit SLP auszuführen, die länger dauern, als es das Initialisierungsskript zulässt. Dies führt zu einem erzwungenen Herunterfahren.

So umgehen Sie dieses Problem:

1. Erstellen Sie eine leere Datei mit dem Namen `hosts.nds` im Konfigurationsverzeichnis. Das Konfigurationsverzeichnis eines Servers kann mit dem Befehl `ndsconfig get n4u.server.confdir` abgerufen werden.
2. Setzen Sie die Umgebungsvariable NDS_USESLP auf 0, indem Sie in `/opt/novell/eDirectory/sbin/pre_ndsd_start` die Exportoption NDS_USESLP=0 festlegen.
3. Starten Sie eDirectory neu.

23.25 Neustart von NLDAP unter Windows

Nachdem NLDAP gestoppt wurde, müssen Sie den Server neu starten, um NLDAP zu laden.

23.26 SecretStore über LDAP

Die NetIQ SecretStore-Funktionalität kann über LDAP nicht verwendet werden. Um dieses Problem zu beheben, müssen Sie LDAP über iManager aktualisieren.

23.27 Interoperabilitätsprobleme

23.27.1 Passwortsatz kann nach dem Entsperren von SecretStore nicht geändert werden

SecretStore wird gesperrt, wenn Sie versuchen, ein vergessenes Passwort abzurufen, indem Sie sich mit der Benutzerberechtigung anmelden und ein falsches Passwort verwenden. Sie entsperren SecretStore mit der Administratorberechtigung. Der NetIQ SecureLogin-Client ermöglicht die Anmeldung ohne Passwortsatz. Beim Versuch, die Passwortfrage und -antwort zu ändern, schlägt die Anmeldung fehl und es wird eine Fehlermeldung ausgegeben.

23.27.2 Die über SecretStore geänderten Benutzerberechtigungen werden auf Null zurückgesetzt

Wenn Sie die neuen Berechtigungen im SecretStore speichern, wird eine leere Berechtigungsspalte angezeigt, weil iManager die Änderungen nicht speichert.

Sie können die Berechtigungen aus dem SecretStore iManager-Plugin nur ändern, wenn Sie sich als Benutzer statt als Administrator anmelden.

23.27.3 Beim Erstellen eines anderen Berechtigungssatzes mit demselben Benutzer wird der vorherige Berechtigungssatz überschrieben

Wenn Sie die alternativen Berechtigungen speichern, behält SecretStore die ersten Berechtigungen nicht bei. Nur die neuesten Berechtigungen sind sichtbar.

Sie können die Berechtigungen aus dem SecretStore iManager-Plugin nur ändern, wenn Sie sich als Benutzer statt als Administrator anmelden.

24 IPV6

Dieser Abschnitt enthält Informationen zur Behebung von IPv6-Problemen auf beliebigen Plattformen.

24.1 Die sichere LDAP-Suche funktioniert mit IPv4 und IPv6, nicht jedoch mit beiden

Bei der sicheren LDAP-Suche tritt ein Fehler auf, wenn die Client-Adresse sowohl über IPv4- als ausch IPv6-Adressen verfügt.

24.2 ICE-Plugin funktioniert nicht für die IPv6-Adressen´

Bei der Verbindung zum angeforderten Server tritt folgender Fehler auf, wenn iManager nur IPv4-Adressen überwacht:

```
Unable to connect to the requested server. Verify the name/address and port.
```

Um IPv6 zum Funktionieren von iManager mit eDirectory zu konfigurieren, aktivieren Sie IPv6 mit den folgenden Schritten:

1. Legen Sie die folgenden Eigenschaften in der Datei `catalina.properties` fest und starten Sie Tomcat neu.

   ```
   java.net.preferIPv4Stack=false
   ```

   ```
   java.net.preferIPv4Addresses=true
   ```

   Beachten Sie, dass `java.net.preferIPv4Stack` für das Funktionieren von iManager mit eDirectory und `java.net.preferIPv4Addresses` für das Funktionieren von Browsern mit iManager gilt.

2. Wechseln Sie zu *LDAP-Optionen* > *LDAP-Server anzeigen* > *Verbindungen*> *LDAP-Server* und fügen Sie LDAP-Schnittstellen für die IPv6-Adressen mit den Portnummern hinzu.

   ```
   ldap://[xx::xx]:389
   ldaps://[xx::xx]:636
   ```

3. Konfigurieren Sie die rollenbasierten Services, melden Sie sich dann von der Sitzung ab und melden Sie sich erneut an.

24.3 Listener für nicht festgelegte IPv6-Adressen in Linux und Windows

Ein Listener für eine nicht festgelegte IPv6-Adresse akzeptiert unter Linux sowohl IPv4- als auch IPv6-Verbindungen. Aufgrund dieses Verhaltens lässt Linux nicht zu, dass nicht spezifizierte IPv4- und IPv6-Listener zur gleichen Zeit den gleichen Port überwachen. Wenn daher ein Listener bereits für eine nicht spezifizierte IPv6-Adresse konfiguriert ist, tritt beim Starten des Listener an der nicht festgelegten IPv4-Adresse ein Fehler auf. Linux verwendet eine nicht spezifizierte Adresse für LDAP-Listener.

HINWEIS: Wenn auf einem SLES 10-Computer bereits ein nicht spezifizierter IPv4-Listener vorhanden ist, werden die IPv6-spezifischen Listener für den gleichen Port nicht gestartet. Dies ist ein bekanntes Problem unter SLES 10. In SLES 11 tritt dieses Problem jedoch nicht auf.

Unter Windows akzeptiert ein nicht festgelegter IPv6-Listener nur IPv6-Verbindungen. Daher muss ein getrennter IPv4-Listener konfiguriert werden, um IPv4-Verbindungen zusammen mit IPv6-Verbindungen zu akzeptieren.

Standardmäßig sind für ldapInterfaces sowohl IPv4- als auch IPv6-Listener konfiguriert. Je nach Plattform startet ldapInterfaces die erforderlichen Listener.